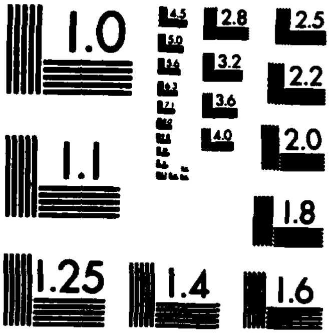
AD-A181 462 APPLICABILITY OF ARMY AUTOMATION SECURITY GUIDANCE TO 1/2
LOCAL AREA COMPUTER NETWORK SECURITY(U) NAVAL
POSTGRADUATE SCHOOL MONTEREY CA J D AYRES MAR 87
UNCLASSIFIED F/G 12/8 NL


1.0
4.5
5.0
5.6
6.3
7.1
2.8
3.2
3.6
4.0
2.5
2.2
2.0
1.1
1.8
1.25
1.4
1.6

2

NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

APPLICABILITY OF ARMY AUTOMATION
SECURITY GUIDANCE
TO
LOCAL AREA COMPUTER NETWORK SECURITY

by

Jeffrey D. Ayres

March 1987

Thesis Advisor Thomas J. Brown

Approved for public release; distribution is unlimited.

A181462

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION
UNCLASSIFIED

1b RESTRICTIVE MARKINGS

2a SECURITY CLASSIFICATION AUTHORITY

2b DECLASSIFICATION / DOWNGRADING SCHEDULE

3 DISTRIBUTION / AVAILABILITY OF REPORT
Approved for public release;
distribution is unlimited.

4 PERFORMING ORGANIZATION REPORT NUMBER(S)

5 MONITORING ORGANIZATION REPORT NUMBER(S)

6a NAME OF PERFORMING ORGANIZATION
Naval Postgraduate School

6b OFFICE SYMBOL *(If applicable)*
Code 62

7a NAME OF MONITORING ORGANIZATION
Naval Postgraduate School

6c ADDRESS *(City, State, and ZIP Code)*
Monterey, California 93943-5000

7b ADDRESS *(City, State, and ZIP Code)*
Monterey, California 93943-5000

8a NAME OF FUNDING / SPONSORING ORGANIZATION

8b OFFICE SYMBOL *(If applicable)*

9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

8c ADDRESS *(City, State, and ZIP Code)*

10 SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO	PROJECT NO	TASK NO	WORK UNIT ACCESSION NO

11 TITLE *(Include Security Classification)*
APPLICABILITY OF ARMY AUTOMATION SECURITY GUIDANCE TO
LOCAL AREA COMPUTER NETWORK SECURITY

12 PERSONAL AUTHOR(S)
Jeffrey D. Ayres

13a TYPE OF REPORT
Master's Thesis

13b TIME COVERED
FROM ______ TO ______

14 DATE OF REPORT *(Year, Month, Day)*
1987 March

15 PAGE COUNT
135

16 SUPPLEMENTARY NOTATION

17 COSATI CODES

FIELD	GROUP	SUB-GROUP

18 SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*
Computer network security, Local area network security, Army computer network security regulations, guidance, regulations, security.

19 ABSTRACT *(Continue on reverse if necessary and identify by block number)*

The U.S. Army Combat Developments Experimentation Center (USACDEC) Directorate of Information Management (DIM), Fort Ord, is currently involved with several network implementations, all at various stages of development, and wants adequate network security at an affordable price. During early stages of development they found almost no existing local area network (LAN) security guidance. This thesis does not look for a set or perfect LAN guidance solution, but develops a background for security considerations during the development of a network based on existing automated data processing security guidance. All Army guidance reviewed was supplied by USACDEC/DIM; all other (DoD, etc.) guidance was selected for review by USACDEC/DIM, but obtained else where.

Theses),

20 DISTRIBUTION / AVAILABILITY OF ABSTRACT
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS

21 ABSTRACT SECURITY CLASSIFICATION

22a NAME OF RESPONSIBLE INDIVIDUAL
Thomas J. Brown

22b TELEPHONE *(Include Area Code)*
(408) 646-3117

22c OFFICE SYMBOL
Code 62Bb

83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

Applicability of Army Automation Security Guidance to Local Area Computer Network Security

by

Jeffrey D. Ayres
Captain, United States Air Force
B.B.A., University of Wisconsin - Eau Claire, 1979

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY
(Command, Control and Communications)

from the

NAVAL POSTGRADUATE SCHOOL
March 1987

Author: Jeffrey D. Ayres
Jeffrey D. Ayres

Approved by: Thomas J. Brown, Thesis Advisor

Peter J. Blakney Jr., Second Reader

Michael G. Sovereign, Chairman,
Joint Command, Control, and Communications Academic Group

David A. Schrady,
Academic Dean

ABSTRACT

The U.S. Army Combat Developments Experimentation Center (USACDEC) Directorate of Information Management (DIM), Fort Ord, is currently involved with several network implementations, all at various stages of development, and wants adequate network security at an affordable price. During early stages of development they found almost no existing local area network (LAN) security guidance. This thesis does not look for a set or perfect LAN guidance solution, but develops a background for security considerations during the development of a network based on existing automated data processing security guidance. All Army guidance reviewed was supplied by USACDEC/DIM; all other (DoD, etc.) guidance was selected for review by USACDEC/DIM, but obtained else where.

TABLE OF CONTENTS

LIST OF FIGURES

I. INTRODUCTION: OVERVIEW OF A LOCAL AREA COMPUTER NETWORK SECURITY ENVIRONMENT

A. INTRODUCTION

1. The Military Computer Security Threat

Computer security is a problem that plagues many computer centers. Computer security is especially important in the military where extensive automated data processing (ADP) systems control large forces and sensitive information. Moreover,

> the potential damage from penetration is growing with the ever increasing concentration of sensitive information in computers and the interconnection of these computers into large networks. Through computer penetration an enemy could, for example, compromise plans for employment of tactical fighters or compromise operational plans and targeting for nuclear missiles. [Ref. 1: p. 17]

For example, one group of juvenile hackers "managed to shift the orbit of one or more communications satellites." [Ref. 2: p. 13] In terms of control of military forces, this type of penetration via computer could be a serious event in a command, control and communications (C3) context because C3 systems include computers, satellites and communications hardware. Thus, C3 computer networks, as well as other military systems, must continually operate in a secure manner.

C3 networks and other military systems include computer networks, local networks, and local area networks (LAN). A computer network consists of one or more computers with the connected terminal devices and other related devices, such as modems and input/output channels [Ref. 3: p. 258]. A local network is a "small-area" communications network that provides interconnection for a variety of data communication devices. Moreover, a LAN is a "general-purpose local network that can serve a variety of devices and is typically used for terminals, microcomputers, and minicomputers." [Ref. 4: p. 296] Given the preceding definitions, this thesis will consider a local computer network (LCN) and a LAN one in the same.

Before addressing security of LANs, a C3 environment is addressed to provide an example and background of distributed processing.

2. Overview of LANs in a C3 Environment

This section will provide a general definition of C3, a definition of distributed processing, a look at LAN support of distributed processing, some C3 environmental considerations for LAN, and lastly, a few C3 functional activities and applications.

Many varied definitions of C3 exist; not all are agreed upon in military circles. There are variations such as command and control (C2) alone; C3; command, control, communications and intelligence (C3I), etc. [Ref. 5: pp. 1-6]. For the purpose of this thesis the following definition from JCS Pub. 1 will be used.

> The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of his mission. Command and control functions are performed through an arrangement of personnel, equipment, communication, facilities, and procedures which are employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of a mission. [Ref. 5: p. 6]

Thus, a C3 system is used to support a decision maker (commander). Moreover,

> sensors, automatic data processors (ADP), and communications equipment and systems are extensions of the decision maker's ability to gather, process, and disseminate information. [Ref. 6: p. 618]

For our purposes C3 will be used in a general way to indicate any type of command and control (C2, C3, C3I, etc.) system.

Given the above comments, a C3 system generally consists of human, sensor, communication and ADP components, along with any associated software. This thesis will only consider the ADP network aspects that relate to C3 in general. All man-in-the-loop and sensor considerations are ignored in this thesis because it deals strictly with LAN security. C3 is used as an application example because it is one military application that often involves distributed processing supported by computers and networks.

C3 systems tend to be distributed configurations. Distributed processing is implemented via communications and computer networks. Current trends in C3 systems are toward surviveable dispersed systems in which distributed ADP will play a major role [Ref. 6: p. 638]. Distributed ADP is "data processing in an organization where some or all of the processing and storage of data is provided at different locations that are connected by telecommunication lines." Decentralized ADP is "data processing in an organization where the processing and storage of data are provided independently at various locations throughout the organization." Any distributed computer system can support both types of processing. A combination of both can be used in a C3 system [Ref. 3: pp. 114,127]. Furthermore, pure distributed data management involves the increased sharing of responsibility (with users) for managing functions of processing, movement, and storage of information. The overall approach of distributed system development is "to develop a conceptual view. . . to provide a framework in which to manage distributed data management." [Ref. 7: pp. 6-8]

Distributed processing can be viewed as a hierarchical structure of computer systems and LANs. In this context, a local area network (LAN) will refer to a physically separate geographic part of a distributed computing/communications system. It includes an interconnection of computer processors, terminals, sensors, etc., and the required software. Normally, all LAN components are channeled through a central point to communicate with other LANs and wide area networks, however multiple control points are possible [Ref. 8]. Moreover, individual computer systems make up LAN configurations. In the broader sense, the computer system supports some kind(s) of functional application(s) through application software. The LAN also supports applications, only in a distributed environment.

> LANs have emerged as the practical way to evolve yesterday's centralized, time sharing computer system into tomorrow's truly distributed network of functionally dedicated, microprocessor based servers.

Thus, LANs can be thought of as the "system bus" for locally distributed computing environments [Ref. 9: p. 69]. In other words, transfering data within the distributed LAN environment is similar to the transfer of data within a single computer system.

The general environment a C3 system operates in is one in which "the rate, complexity, dimensionality, and uncertainty of events and of information about them, in both crisis and war situations, is rapidly increasing." Understanding of events and force information is required for effective force management [Ref. 6: p. 620]. Thus, a commanders mission performance depends on his C3 system [Ref. 10: p. 87]. To all that, computers can and are used to provide a qualitative superiority in areas were we are outnumbered. For example, computers are at the heart of the C3 process in the Air Force. The need for secure computer networks

> is clear when we realize that good C3 capabilities can double or triple force effectiveness: conversely, ineffective C3 is certain to jeopardize or deny the objective sought. [Ref. 1: pp. 17-18]

Generally, the driving force behind LAN and ADP security is to reduce or eliminate potential damage from unauthorized system penetration. For example, given the Walker spy ring incident, consider this scenario: a Soviet agent aboard a U.S. Navy warship stealing the ship's ability to fight by tampering with sensor and weapon software. An agent would accomplish this by inserting or modifying portions of software modules. "Like an invisible time bomb, the subverted software could lie hidden in the computer system, ready to explode in the form of catastrophic commands." [Ref. 2: p.12]

Given the processes/activities within a C3 system,

> information technology does not simply help the commander and his staff, but also stimulates the development of collective military creativity, in which the largest group of people, including those separated by great distances, can participate (in Druzhinin and Kontorov). [Ref. 6: pp. 619-620]

As a result, a LAN can help provide filtering in a wide variety of processing; from data collection to decision aids. Some examples include dynamic electronic maps, pointers and blackboards. [Ref. 6: pp. 627,636]

In short, various "Department of Defense (DoD) computers handle virtually everything from targeting ICBM's to parceling out spaces in the Pentagon parking lot." [Ref. 2: p. 1] Given that "the flexibility of LANs for dynamic system expansion and reconfiguration is particularly applicable to tactical C3I applications," the future should bring more advanced ADP networks supporting C3 with more versatile and accurate resolution and filtering. [Ref. 9: p. 69]

3. LAN Security Problems

Earlier we mentioned some examples of LAN penetration that indicate security is especially important in the C3 arena. However, it is important to all government systems in general. Many government and military C3 systems depend on some form of a LAN configuration. Thus, we will concentrate on small local level military LAN configurations with emphasis on security at the unit level. This section will address a few general computer network security points in terms of ADP target areas, espionage and internal vulnerabilities.

General ADP target areas include electronic emissions, loose personnel procedures, network interfaces, operating systems and physical access. Once an ADP/network target area is chosen, a system penetration can result in [Ref. 11: p. 81]:

- Observation - no direct effect in, or change in data.
- Extraction - copying data.
- Alteration - modification or change of hardware, procedures, or data.
- Addition of extraneous data.
- Use of hardware or software resources.

The above penetration activities can result in "espionage". It can be internal, like the Walker spy ring, or external from enemy sources and hackers. For example, a UCLA student broke into over 150 computer accounts in the Pentagon funded Advance Research Project Agency Network (ARPANET) [Ref. 2: preface]. Moreover, in an attempt to prove system security, Air Force tiger teams have penetrated Air Force systems which were thought to be tamper-proof. Tiger team findings and comments include:

- New teams found new holes, even after previous teams could not gain access.
- Holes generally result from human design oversight.
- It does not take a highly skilled expert to penetrate security.
- The access threat from outside sources is growing; communication tabs; microwave intercepts; etc. [Ref. 1: pp. 23-24]

Some common techniques used to commit computer-related fraud and abuse are listed below.

- COMPUTER-RELATED FRAUD
  - Entering unauthorized information
  - Manipulating authorized input information
  - Manipulating or improperly using information files and records
  - Creating unauthorized files and records
  - Overriding internal controls.
- COMPUTER-RELATED ABUSE
  - Stealing computer time, software, information, or equipment
  - Entering unauthorized information
  - Creating unauthorized information files and records
  - Developing computer programs for nonwork purposes
  - Manipulating or improperly using computer processing.

Examples range from routing government funds to personal bank accounts, to selling information. [Ref. 12: pp. 10-11,31]

Obviously, given an application and threats of fraud and abuse, ADP security is required. By consequence, the level of security required for a network must be approved before operations begin. In the Army the ADP and network approval process is called accreditation.

4. Accreditation Process

One important result of concerns for ADP security in the Army is the accreditation process.

> The term 'accreditation' is used to describe the process where by information pertaining to the security of an Army data processing activity (DPA), ATS (automated telecommunications system), or network is collected analyzed, and submitted for approval. [Ref. 13: p. 30]

The accreditation authority for systems processing critically sensitive (CS) levels of information are Headquarters Department of the Army (HQDA) or major command (MACOM) commanders (general officers), depending on the system. For highly sensitive (HS) information, installation, post, or field operation commanders can be the accreditation authority. At the sensitive level the heads of the data processing activities (DPA) or centralized office automation agencies may be the accreditation authority. More on sensitivity, and accreditation is presented in following chapters. Nonsensitive systems do not need accreditation. [Ref. 13: p. 6]

The accreditation authority reviews submitted system documentation and approves or disapproves it. Disapproval indicates that the level of risk associated with the system is not acceptable. The goal is to make sure the accreditation efforts relate to the specified system, and that the system is cost effective. [Ref. 13: p. 30]

The variation in types of systems, functions, and installations caused the Army to develop different accreditation standards and procedures. For example, Army data processing activities (DPA) and/or automated telecommunication systems (ATS) are grouped according to sensitivity categories and levels.

The accreditation process is a critical review of a designated DPA/ATS prior to accreditation. The purpose: "to provide information which will enable the accreditation authority to determine that sensitive information can be processed within the bounds of acceptable risk." By consequence, the analytical accreditation process requires, as a minimum, investigation, information gathering, and formal review by command authorities at both the operating and accrediting levels. Understandably, accreditation evolves from completing a series of goal and objective statements, management reviews, operation and system descriptions, and other documentation and reviews. In addition, all documentation must be classified according to its sensitivity level. [Ref. 13]

The process ends when "a formal, dated, statement of accreditation has been issued by the appropriate authority." At that time the accreditation is effective. [Ref. 13]

B. PURPOSE

The U.S. Army Combat Developments Experimentation Center (USACDEC) Directorate of Information Management (DIM), Fort Ord, is currently involved with several network implementations, all at various stages of development. Like many government agencies, USACDEC has it's own inherent resource constraints, and wants adequate network security at an affordable price. During early stages of development they found almost no existing LAN security guidance. Given their networks would be approved in terms of existing guidance, and their requirement to process sensitive information, USACDEC/DIM was interested in an "outsider's" interpretation of ADP security guidance in terms of LANs. Thus the following thesis statement was developed:

> Identify local computer network (LAN) regulation and guidance requirements that are valid and outdated, and LAN areas that are not adequately covered by current regulations, to give system developers a better feel for security boundaries.

In doing this, the purpose is not to look for a set or perfect solution, but to develop a background for security considerations during the development of a network. It is hoped that this will be used as a guide or a tool for identifying security bounds during system development or expansion. The reason, of course, is that there are parts of regulations and guidance that are left to interpretation. To all that, it is common knowledge that computer technology is constantly changing for the better, assuming it's application is not used by upper command/management levels to "micro-manage." Or, in the ADP context, it is not used by upper level commanders to access detailed information at the work level. In addition, current regulations cannot keep up because many new ideas for regulations and ADP protection "have been sidetracked in the rush to modernize computer systems and continually update software." [Ref. 2: p. 3] As a result, a certain level of risk must be accepted by the system developers and sponsors.

Given the wide variety of computer systems and computer networks that exist within the DoD, a generic baseline system is used as a guide. It consists of basic components that can be found in and on many DoD and Army networks. The purpose here is to provide general technical network background information for configuration security analysis, and give the reader some frame of reference. As a result, the general baseline analysis is in terms of configuration hardware, software, and interfaces at a conceptual level. Hence, the scope of the thesis is limited mostly to configuration security; physical security and operational considerations are limited, and personnel security is only mentioned in certain areas. Furthermore, the thesis is intended to serve as a guide for identifying network guidance requirements for system components and the overall system configuration. The system configuration and component topics are identified in Chapter II.

It is hoped that this thesis will provide the system developer with a guide/tool that will help him/her focus an accreditation effort, develop the system, examine potential expansion alternatives, become aware of operational constraints, and develop possible accreditation methods and strategies.

C. ASSUMPTIONS

The following assumptions are made to help limit the scope of the thesis.

- All comments concerning guidance applicability are restricted to the guidance referenced in this thesis. Note: a list of the guidance can be found in Chapter III. All Army guidance reviewed was supplied by USACDEC DIM; all other (DoD, etc.) guidance was selected for review by USACDEC/DIM, but obtained else where.
- The generic baseline used could be a microcomputer, minicomputer, mainframe computer based network, or any combination.
- Specific brands of software and hardware will not be mentioned unless they are a part of many DoD systems.
- The thesis assumes basic building construction of facilities housing LAN components is adequate.
- A risk management analysis is complete. Risk management is explained in Chapter III.
- A "network" has the same basic functions and requirements as a LAN. Thus any references to a "network" in the guidance, pertains to LANs as well.
- Automated data processing (ADP) is used in a general way to represent computer systems.

- The thesis audience is mostly Army or DoD personnel with an ADP background; Army commanders, managers, or security managers considering installation of a network for the first time; and ADP security managers in general.
- No command-unique regulations or guidance documents are referenced.

D. OVERVIEW OF CHAPTERS

The chapters that follow address the generic baseline configuration, a review of current security regulations and guidance, network development considerations pertaining to security requirements, and potential security approval methodology.

More specifically, Chapter II defines the generic baseline LAN configuration in detail. Hardware that may access the network will be identified. In addition, the system software identified will be based on actual software currently in use on some operational networks. Types of tailor-made and off-the-shelf application software will be identified. Examples of possible applications of a network similar to the generic network will be identified. Moreover, environmental considerations will be addressed in a limited fashion, and physical hardware layout will be restricted to hardware interface relationships (no detailed building or floor-plan layouts).

Chapter III will give an overview of the LAN security considerations for the generic LAN baseline described in Chapter II. What's more, it will categorize security regulations and guidance to determine what currently applies and what is outdated Also, parts of the LAN that are not covered by current regulations will be identified.

Network development considerations pertaining to system high requirements and multilevel requirements are identified in Chapter IV. A general strategy is developed pertaining to the generic baseline system. It addresses regulations that apply, current operations, and future expansion. Furthermore, the relevancy of regulations are considered. Interpretations of the regulations are suggested.

Approval methodology is addressed in terms of accreditation requirements in Chapter V. First, the basic Army accreditation process is outlined and important areas are highlighted. Then, gaps between what security regulations state and what exists in the generic network are considered in terms of the accreditation process. Note that directions for accreditation preparation are not presented; only general strategy considerations.

Finally, Chapter VI presents conclusions and summarizes the areas the thesis examines. Additionally, some recommendations are presented in terms of general protection, important guidance, and future research suggestions.

II. A GENERIC "BASELINE" CONFIGURATION

A. BACKGROUND

1. Introduction

In Chapter I a local network was defined to be a small-area general communications network, in contrast to a LAN which is a general purpose local network that is typically used as a computer network. Thus, the basic configuration concepts are the same for both networks. Even though this thesis is concerned with the automatic data processing (ADP) applications of LANs, other devices that can communicate over a LAN transmission medium (i.e. data communication devices) include sensors (temperature, humidity, security, etc.), telephones, and televisions. Moreover, the geographic scope of a LAN is small, usually serving a building or a group of buildings not covering more than a few tens of kilometers. Two examples are a campus or a military base. [Ref. 4: p. 1]

As a general rule, key characteristics are high data rates, short distances, and low error rate. In a well designed network, additions and replacements can be made with little impact on the other devices on the network. In addition, control of the network can be distributed. [Refs. 4,14]

This chapter will look at configuration components, applications, the environment, and expansion in relation to the generic LAN "baseline."

2. Benefits and Pitfalls

A local network improves the reliability, availability, and survivability of an ADP facility through redundancy. In other words, many separate device nodes and links ensure continued operation when part of the network is damaged or under repair. Other general benefits include:

- Improved system responsiveness/performance.
- Use of a single terminal to access multiple computers.
- Flexibility of equipment location. [Ref. 4: pp. 2-3]

One major pitfall is that the addition of new applications or enhancements risks the introduction of errors and the reduction of performance of the entire system. Other general pitfalls include:

- Interoperability/interface problems with diverse types of equipment. Special format-conversion software may be needed.
- Loss of control -- it is hard to control information, enforce standards, protect and secure, and manage, distributed systems. [Ref. 4: pp. 2-3]

3. Reasons for a LAN

General reasons for implementing a LAN include:

- Resource sharing; transmission of information; economizing on terminals, etc.
- Future transitions to new systems is enhanced because it provides a mechanism to put the old and new computer on the same network.
- Expansion.
- Provide vendor independence (related to expansion).
- Easy to add devices to an existing cable plant. Assuming cable was laid to allow for expansion, i.e. throughout a building. [Ref. 15: pp. 186-187]

The generic base-line network configuration for this thesis (reference Figure 2.1) will be based on a collection of host computers, a computer branch exchange, and Ethernet. Both Ethernet and the computer branch exchange (CBX) control routing and transmission of data throughout the network, and both are explained below. Many Department of Defense (DoD) agencies are currently using these components and a baseline is needed for reference in terms of the security regulation analysis. The collection of host computers could be mini, micro, mainframe, or a combination of any of these, although the exact type of computer is not important for our level of analysis. The base-line configuration is intended to provide a vehicle for a general description of basic LAN components, what they do, how they relate to each other, and how they are applied to a LAN configuration.

B. NETWORK CONFIGURATION COMPONENTS

1. Component Overview

There are components and functions common to all LANs. This section defines and explains basic characteristics and functions for some of the following components:

- Topology
- LAN protocols
- Digital switches and Computer Branch Exchanges (CBX)
- Networking interface
- Internetworking (gateways)
- Transmission media
- Ethernet (because selected for the baseline)

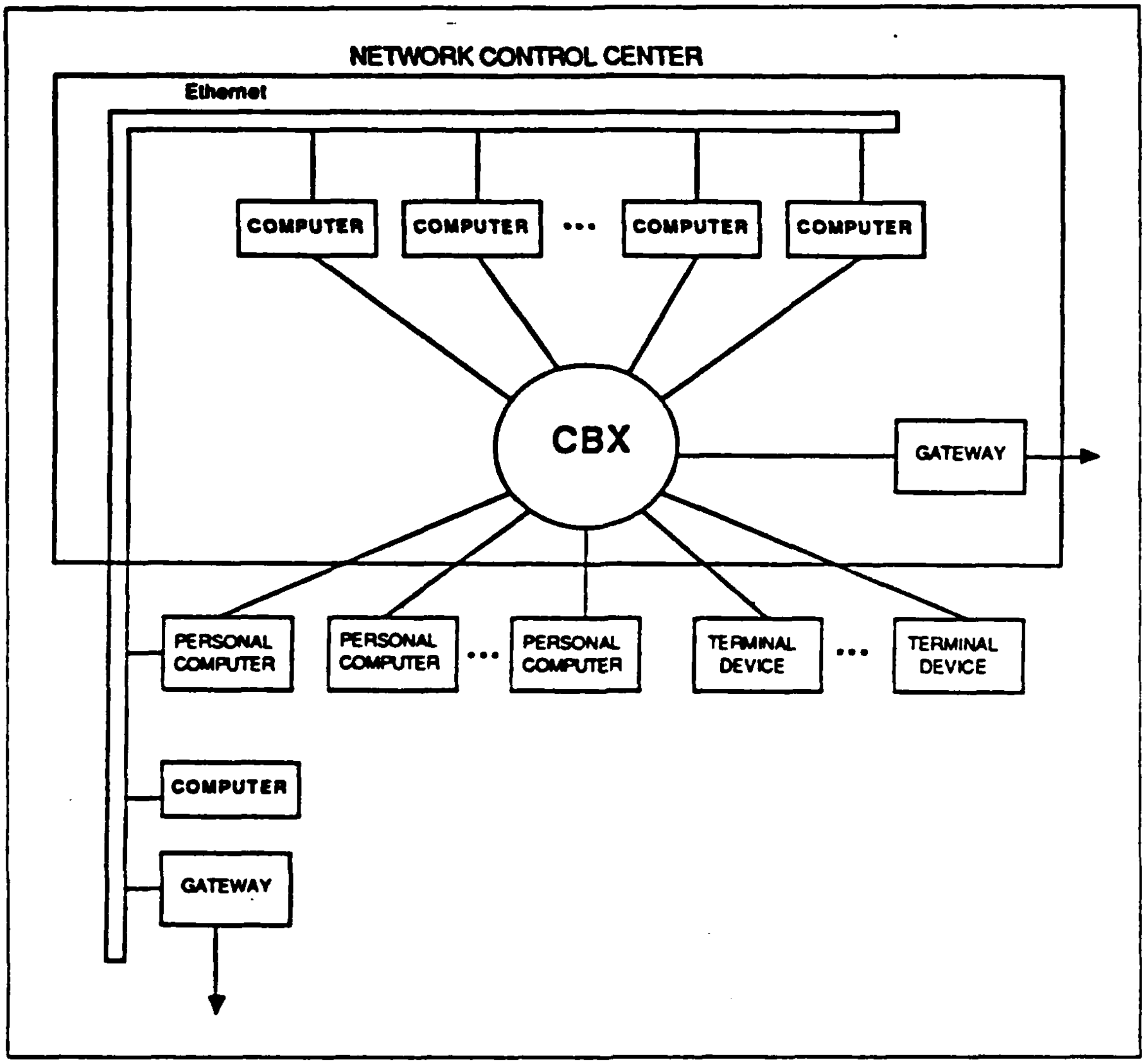


Figure 2.1 Generic Baseline Configuration.

2. Topology

There are three main architectural alternatives for LANs; bus/tree, ring, and star. Reference Figure 2.2 [Ref. 14: p. 10].

a. Bus/tree

In a bus topology the transmission medium is a linear cable shared by all stations and devices. Each station or device is attached to the medium and receives or sends information by bidirectional transmission of signals which propagate the length of the medium [Ref. 4: p. 295]. A tree is also defined as a topology in which stations and devices are attached to a shared transmission medium, but the cable branches out

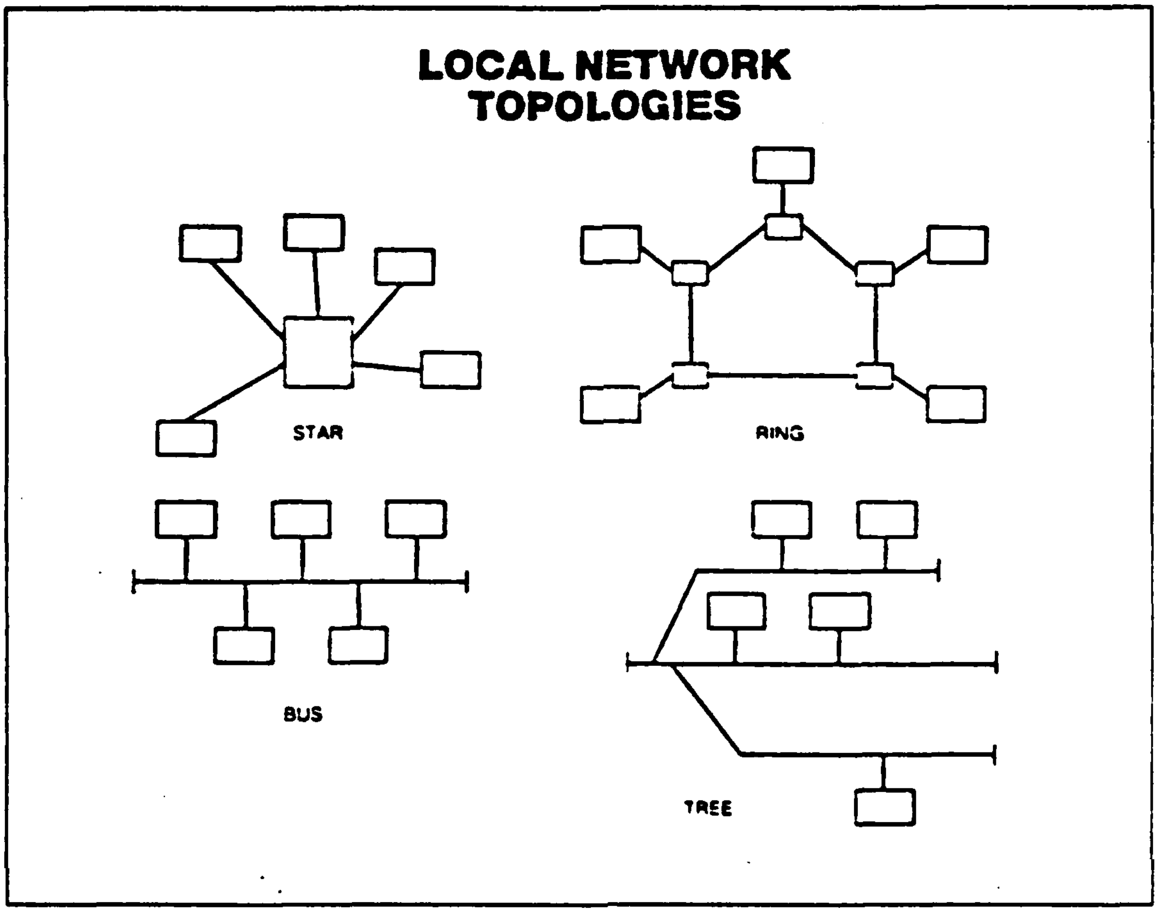


Figure 2.2 Basic Architecture Alternatives.

from a device called a headend. A headend is the end of a multichannel bus or tree network. Stations/devices transmit to, and receive from the headend. The headend enables each station or device to receive and transmit signals among the tree branches [Ref. 4: p. 298]. Bus topologies are usually single channel (baseband); and trees must always be multi-channel (broadband). For a more detailed description of baseband and broadband see *Tutorial Local Network Technology* Section 2 [Ref. 4].

Bus or tree topologies only allow one pair of devices to communicate at a time because all devices share a common communications medium. In terms of transmission media, trees usually use coaxial cable, but sometimes use twisted pair cable for low performance applications. Transmission media will be addressed later in this chapter [Ref. 14: p. 8].

Problems can arise from the shared access nature of the bus or tree topology. One example of a major problem is determining what station should transmit and when. Another problem is adjusting the signal strength to required levels between devices before transmission (signal balancing). These problems are magnified with many different types of devices and their unique characteristics [Ref. 4: pp. 35-36]. Protocols manage some of these problems and are discussed later in the chapter.

b. Characteristics of Ring LANs

For computer-to-computer communications, the ring is often the most efficient topology [Ref. 14: p. 8]. A single closed path is formed when repeaters are connected by unidirectional transmission links [Ref. 4: p. 36]. A repeater is a device that receives data on one communication link and transmits it sequentially, bit by bit, on another link around the ring from one repeater to the next. The repeater is an integral part of the ring topology because it transmits data as fast as it receives it without buffering, and connects linear segments in a ring network. Data is readable by all attached stations/devices. [Ref. 4: p. 297]

Twisted-pair, baseband coaxial, and fiber-optic cables can all be used as transmission media to provide the repeater-to-repeater links. Broadband coaxial, however, could not easily be used because transmitting data on multiple channels requires more than just a repeater. Functionally this would require asynchronous transmitting and receiving, which is more complicated. [Ref. 4: p. 37]

c. Star Topology

All stations are connected to a central switch in a star topology. Any two stations in the LAN communicate via circuit switching. Circuit switching is a communication method that establishes a dedicated communications path to connect two devices through one or more intermediate switching nodes (i.e. circuit switches). Digital data is sent as a continuous stream of bits. Conceptually, a pure star topology only has one switch (see Figure 2.2). As a result, delay is limited to propagation time and channel bandwidth is guaranteed. [Ref. 4: pp. 295,297]

3. LAN Protocols

LANs need a means of controlling access to transmission media so any two devices on the network can control data when required [Ref. 4: p. 37]. Protocols provide this necessary access control so that the network transmission media can be shared. A protocol is defined as

> a set of rules governing the communication and the transfer of data between two or more devices in a communication system: the rules define the handling of certain communication problems, such as framing, error control, sequence control, transparency, line control, and start-up control. [Ref. 3: p. 303]

A protocol is implemented within a LAN via software, firmware, etc., in the associated LAN devices.

In a protocol, the transmission medium access control technique is based on two parameters. The first is the control location ("where"), i.e. centralized or distributed, and the second parameter is "how". In the "where" parameter, a centralized scheme may afford greater control over access, allow logic at each device or station to be as simple as possible, and avoid problems of coordination. On the other hand, a centralized scheme may act as a bottleneck resulting in a single point of failure and a reduction in efficiency. Distributed scheme pros and cons are a mirror image of the above points for the centralized scheme. In both schemes, the "how" parameter is a trade-off among competing factors, such as those of cost, performance, and complexity. Thus, the parameters are constrained by the topology of the particular centralized or distributed network scheme. [Ref. 4: p. 37]

In all common medium access control techniques, multiple data transfers share a single transmission capacity. The most common access method for LANs is the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) in the random access category, token bus for bus and tree systems, and token ring for rings. [Ref. 4: p. 37]

CSMA/CD operates as follows. Traffic already on the network channel has priority, and only one station can transmit at a time. Each station on the bus listens and waits until the channel is clear before transmitting. Collisions occur when two stations try to transmit at the same time. When collision occurs, both stations will detect it and cut short the transmission, then wait a short period of time before trying another transmission. [Ref. 14: pp. 9-10]

Token bus is a more complicated medium access protocol than CSMA/CD. In token bus, stations on the bus form a virtual ring where each station is assigned a position in an ordered sequence. The first station transmits to any or all the other stations. When the first station is done it passes a control token to the next station in the sequence. This process continues for all stations, and then repeats. [Refs. 3,14: pp. 276-277,10]

Token ring works in a way similar to token bus except the control token is constantly circulating. Transmission is possible only if a station has the control token. Thus, when a station wants to transmit, it grabs the control token, and then returns the control token to circulation when it is finished. [Ref. 14: p. 10]

4. Digital Switches and Computerized Branch Exchange (CBX)

A computerized branch exchange (CBX) is a combination of digital switching and telephone private branch exchange (PBX) technologies. The CBX is defined as "a digital PBX that also handles data devices without modems." Usually a digital switch refers to a system that only handles data over a star topology LAN. A PBX is a telephone exchange on the user's premises that provides a switching facility for telephones on extension lines within a building or local area. In addition, it provides access to the public telephone network. Modern digital PBX characteristics include:

- Use of digital phones to permit integrated voice/data workstations.
- Distributed architecture. Multiple hierarchical switches with distributed intelligence.
- Dedicated port assignments for all attached devices.

Thus, a modern PBX can be used for local area computer networks. This thesis will refer to all modern CBXs and PBXs together as "CBXs". [Ref. 4: pp. 134,295,297]

a. Characteristics

The CBX and the digital switch are major LAN alternatives for handling a wide variety of local networking requirements. One of the most important characteristics is that the stations are usually connected by twisted pair to a central switching unit (star topology). The CBX uses circuit switching to establish a dedicated communications path between two devices wishing to communicate and guarantees the data rate, or "bandwidth". Moreover, while data rates may be limited (64 Kbps), total capacity (throughput) can be high (500 Mbps) [Ref. 4: p. 133]. Even though higher throughput limits can be achieved with a bus or a ring topology, a key distinguishing feature of the CBX is the transparency which it offers due to circuit switching [Ref. 14: p. 10].

A digital switch differs from a CBX in that it only handles data traffic and not voice traffic. Digital switching techniques have been used to build many digital switching products designed for data-only applications, i.e., a digital switch does not provide telephone service. In sum, the major function of a digital switch is to make a connection between two attached lines This is accomplished via two sub-functions.

The first is port contention which is used for host-to-terminal connections when a limited number of ports are open for a larger number of terminals. The second sub-function, port selection, is an interactive process of allowing an application program or user to select a specific port or connection. If the switch did not allow this capability, only connections that were pre-configured by a system operator would be possible. Notice that for brevity, we have assumed that the control unit of the switch can talk to the requesting port. [Ref. 4: p. 133]

b. Architecture

Manufacturers have developed a variety of CBX architectures. They are proprietary, so the details are not generally available in most cases. Thus, the general architectural features common to all CBX systems will be presented. [Ref. 4: p. 134]

Figure 2.3 illustrates a generic CBX architecture. Note that the CBX degenerates to a digital switch architecture if you eliminate the voice features. [Ref. 16: p. 237]

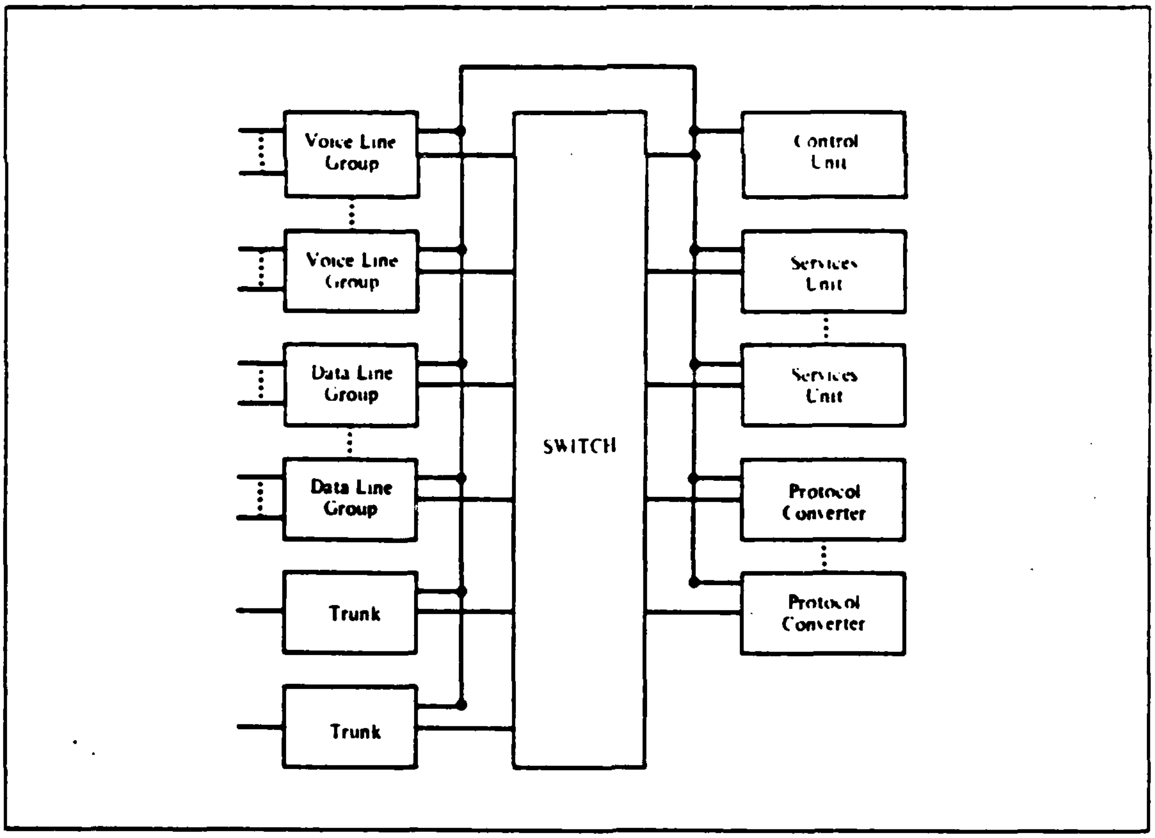


Figure 2.3 Generic CBX Architecture.

The heart of the system is a digital switching network that has a series of interface units attached. They provide access to or from the outside world. Multiple incoming lines (usually 8-24) are multiplexed by the interface unit for input to the switch. The control unit exchanges control signals with attached devices and operates the digital switch. Service units include dialed-digit registers and tone and busy-signal generators. A trunk is a communications channel between two switching centers that normally consists of a group of lines enclosed in a single casing. Trunk interface units are used to connect off-site locations, and protocol converters connect dissimilar lines. [Refs. 4,16: pp. 134-136,566]

This generic architecture is reliable because the failure of any interface unit means the loss of only a small number of lines. Key elements like the control unit can be made redundant. [Ref. 4: p. 136]

5. The Network Interface

All network devices must share a common LAN protocol to be compatible. There are three general ways that devices can attach to a LAN. The first is the "homogenous/single-vendor approach" where everything is guaranteed to be compatible by the vendor. In other words, each device can physically connect and operate with minimal interface software and handle the same protocol. Second, is the "'standards' approach". The standards approach is an interconnection problem because current standards tend to freeze technology when new interfaces are developed. Furthermore, new standards for interfaces are constantly on the drawing boards and often become obsolete as soon as they are issued [Ref. 16: p. 121]. Last, is the "standard network interface approach" in which network operation details are hidden from the device [Ref. 4: p. 173]. Given the various ways to make LAN interconnections, some sort of network interface unit (NIU) is required to attach a device/station to a LAN.

Typically, the NIU is a microprocessor-based device that functions like a communications controller to provide data transmission service to the attached device. General NIU functions include:

- Accept data from connected device.
- Buffer the data until medium access is obtained.
- Transmit addressed data packets.
- Search for packets on the medium that have the device's own address.
- Load the packet into buffer.
- Transmit data (at the proper data rate) to the attached device.

Usually the hardware interface between the NIU and the attached devices is a standard serial communications interface such as RS-232C. In data communications, the RS-232-C is a set of standards specifying various electrical, mechanical, functional, and procedural characteristics for interfaces between computers, terminals, and modems. The NIU can be an outboard device (a stand alone unit) or an inboard device (one or more circuit boards attached to the device's bus). Another important characteristic of the NIU is that it must, at a minimum, implement the LAN protocol. A generic NIU model is depicted in Figure 2.4. [Refs. 3,4,15,16]

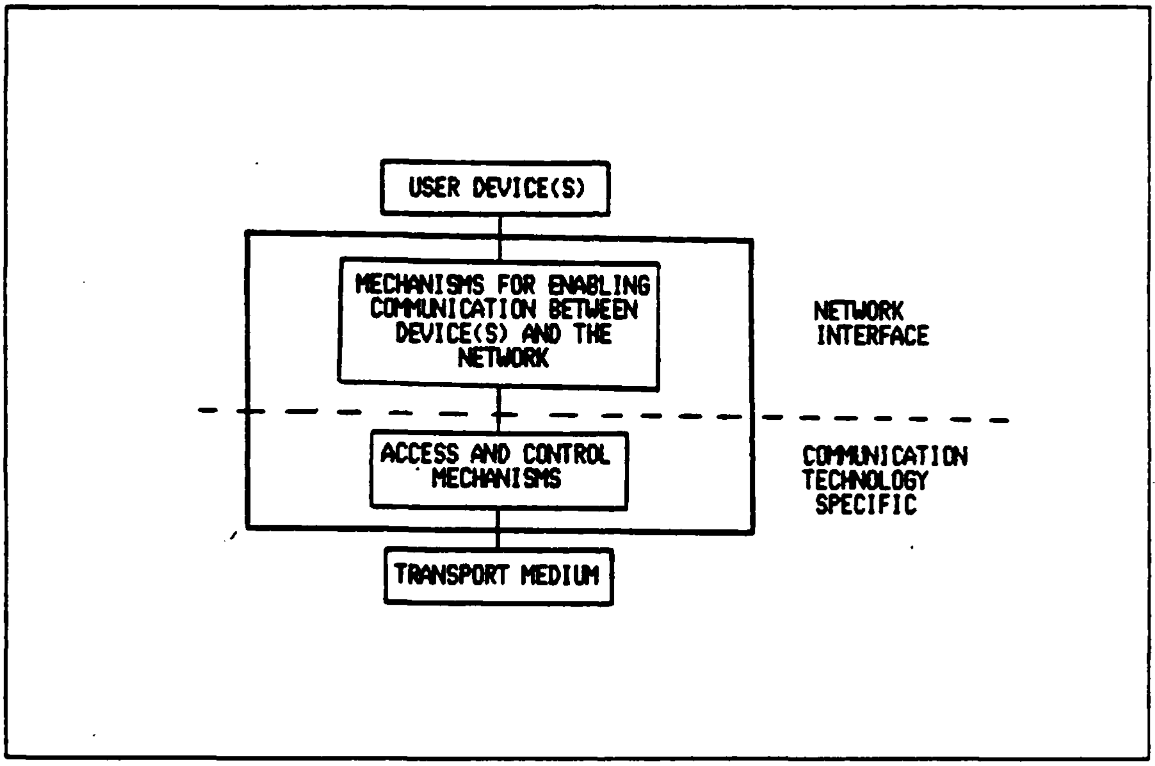

USER DEVICE(S)
MECHANISMS FOR ENABLING COMMUNICATION BETWEEN DEVICE(S) AND THE NETWORK
NETWORK INTERFACE
ACCESS AND CONTROL MECHANISMS
COMMUNICATION TECHNOLOGY SPECIFIC
TRANSPORT MEDIUM

Figure 2.4 The Generic Interface Model.

6. Internetworking

Internetworking is the communication among devices on two or more networks. The bridge and gateway are two common methods used to provide internetworking. The simplest is the bridge because it is for homogeneous local networks, i.e. the same interfaces and protocols. Typically, it is used for network interconnections involving one-vendor hardware. This thesis will focus on the more complicated gateway. Reference Figure 2.5. [Refs. 4,16]

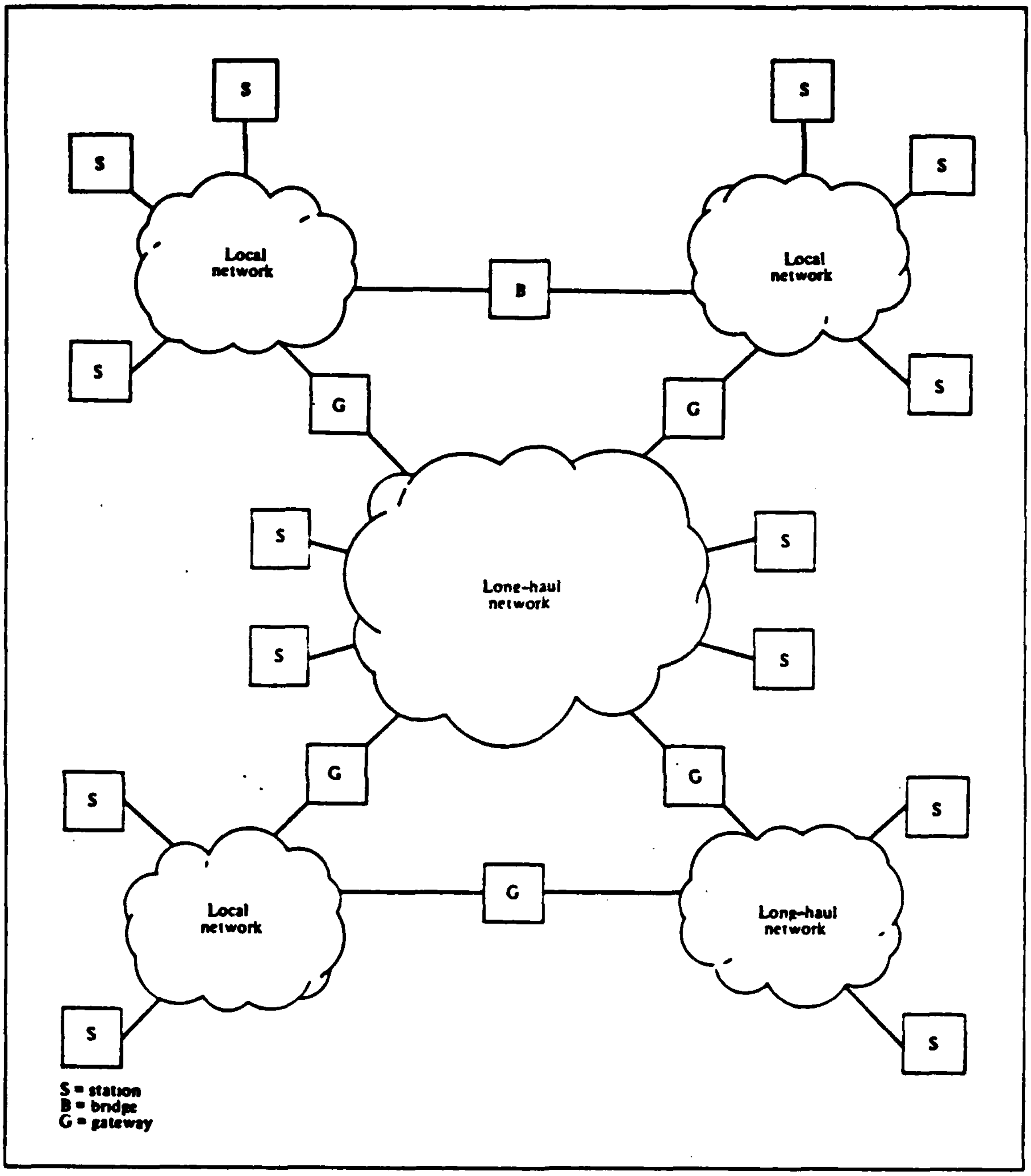


Figure 2.5 Interconnected Networks (Catenet).

A gateway is a device that connects two systems, usually systems that use different protocols. For instance, a gateway would be used to connect two independent local networks or to connect a local network to a long-haul network. As a result, a gateway device is complex because it must accommodate differences between networks (local and long-haul). These differences include: addressing schemes, maximum packet size, network interfaces, time-outs, error recovery, status reporting, routing techniques, access controls, and connections. Thus, protocols are the major cause of gateway design issues. [Ref. 4: pp. 229-231,296]

Different protocol approaches can be used to accommodate these network differences. In fact, a different gateway must be built for each pair of networks, which is hard to manage from an internetwork standpoint. In contrast, an internet protocol (IP) is a better approach. The idea behind the IP is that the gateways and stations share a common protocol only for internetwork traffic, while normal intranetwork operations are undisturbed. This enables one to eliminate internetting capabilities from the local network and puts the burden for the IP on the gateway. Additionally, the IP concept is taken one step further in a catenet which is a collection of interconnected networks using an IP. [Refs. 4,15]

7. Transmission Media

A transmission medium is defined as the physical path between network transmitters and receivers in a communications system. Common media include twisted pair cable, coaxial cable, radio waves, optical fibers, and infrared transmission through the atmosphere. The geographic scope of these media is the maximum distance between different points on the network. Noise is a contamination of the network that includes effects of distortion and interference. Different media have varied immunity to noise, due to their construction and nature of operation. [Ref. 17: pp. 19,21]

Traditionally, twisted pair, coaxial, and fiber optic cables are used to transmit information within a LAN and are the media our generic configuration will use. Understandably the physical channel produces certain constraints on factors important to the network manager in terms of the amount and quality of information transmitted. [Ref. 17: p. 21]

a. Twisted Pair

Twisted pair is just that, a pair of wires that form a transmission line/cable. The transmission distance depends on signaling techniques and quality of wire. Twisted pair can be used for both multipoint and point-to-point in analog or digital transmission. Moreover, multipoint service data rates and distance are restricted. In addition, twisted pair provides one data path known as the "baseband", which consists of a bidirectional digital signal [Ref. 16: p. 32]. Usually twisted pair is used for low speed transmissions. In short, point-to-point is better than multipoint for LAN applications, and most applications restricted to buildings or a few close buildings. Furthermore, extra protection is required for twisted pair, especially when it runs outside buildings. [Refs. 14,17: pp. 7,22-23]

Geographic scope is an important parameter in terms of network security for twisted pair. The reason is that energy loss increases with distance between devices. What's more, the transmission line acts like a transmission antenna and allows motivated outsiders to detect and receive that energy. Under the right conditions normal LAN transmission distances can range up to 15 kilometers. [Refs. 14,17: pp. 7,22-23]

The CBX is the most common contemporary network implementation using twisted pair transmission lines among network nodes. Hence, twisted pair connections are usually from device to central switch, intermediate switch, or multiplexer. [Ref. 17: p. 23]

b. Coaxial Cable

Construction of coaxial cable is more complicated than twisted pair. There is an internal conductor wire with an outer conductor concentric with and completely surrounding it. Coaxial cable is used for point-to-point applications. Besides that. it is particularly good for multipoint topologies, yet it can be used for simple to sophisticated conventional topologies (star, ring, bus, etc.), and variations of the above. In fact, coaxial cable networks are well suited to bus/tree architectures, that may be used for office automation, laboratory, and process control environments. [Ref. 17: pp. 24-26]

Both baseband and broadband coaxial transmission distances depend on tolerable delay, load, and implementation. Unlike baseband, broadband provides multiple and separate data paths (channels). Maximum distances in typical baseband coaxial networks are limited to one to three kilometers, while broadband networks can span areas of ten kilometers or more (fifty is a practical upper limit). Capacity is mid-range between twisted pair and fiber optic cable (fiber optic is covered next). In short, broadband coaxial cable can provide a high throughput for a large number of devices. [Refs. 14,17: pp. 7,25]

Even though coaxial cable has a different construction than twisted pair, it may still "act as an antenna allowing an eavesdropper to tap into the line with pickup coils appropriately placed." As a result, geographic scope is an important network security parameter for coaxial cable. [Ref. 17: p. 24]

c. *Fiber Optics*

Compared to conventional twisted pair and coaxial media, optical fiber has a completely different construction and composition. One optical fiber has a center core of plastic or glass material with a high index of refraction. Each fiber is surrounded by a cladding layer of a material with a slightly lower index of refraction. The cladding layer isolates the fibers and prevents cross talk between adjacent fibers. An optical cable consists of a group of discrete optical fibers that each transmit a light signal from one end of the cable to the other. [Ref. 17: p. 26]

Some fiber optic cables include a steel stabilizing central member. This type of cable should be avoided in applications where computer security is of importance because the steel stabilizer acts as an antenna for the signals, even though fiber cable does not use the steel stabilizer for transmission. Without a steel stabilizer, fiber optic cable is tap proof because the number of passive taps are currently limited by the properties and composition of the cable. So in relation to network security, fiber optic cable can provide a non-emanating media that requires less physical protection than twisted-pair or coaxial cable. [Ref. 17: pp. 27-29]

A signal-encoded beam of light is transmitted through an optical cable to produce high transmission capacities. Data rates are as high as a few gigabits per second over a single glass fiber. [Ref. 17: pp. 26-27]

Current applications include long-haul computer-to-computer high speed links, long distance terminal and processor connections, links between buildings, and communications trunks between complexes at opposite ends of a city. [Ref. 17: p. 28]

8. Ethernet

Ethernet is a packet switched, multi-accessed communications system for carrying digital data among locally distributed computing systems. It is a passive broadcast medium with no central control for the network communication channel. Channel access is coordinated in a distributed fashion by the stations wishing to transmit. Ethernet was originally developed by Xerox. The current updated version of the Ethernet design was jointly developed by Digital Equipment Corporation, Intel, and Xerox. [Ref. 18: p. 39]

Ethernet access techniques are based on CSMA/CD (mentioned above). The basic components consist of a station, controller, transmission system, and controller-to-transmission-system interface. The "station" is the basic addressable device connected to an Ethernet; it may be a terminal, computer, or some other ADP device.

As a general rule, the set of functions and algorithms needed to manage access to the channel are referred to as the controller. The transmission system includes a broadcast transmission medium, the appropriate transmitting and receiving devices, and all the components used to establish a communications path among the controllers. The Ethernet interface is fairly simple because the controller does much of the work. For instance, the protocol for managing access to the transmission system is implemented in the controller, and the controller manages the communications process. [Ref. 18: pp. 40,44]

Applications intended for Ethernet include office automation, distributed data processing, and terminal access. The driving force behind it's development was to provide economical connection to a local communication medium carrying bursts of traffic at high peak data rates. [Ref. 18: p. 53]

Security of Ethernet systems is summarized:

> Protection, security, and access control are all system-wide functions that require a comprehensive strategy. The Ethernet system itself is not designed to provide encryption or other mechanisms for security, since these techniques by themselves do not provide the kind of protection most users require. Security in the form of encryption, where required, is the responsibility of the end-user processes. [Ref. 18: p. 53]

9. The Generic Base-line Configuration

As mentioned above, the configuration illustrated in Figure 2.1 is used for illustration only. It represents the majority of basic components typical of LAN applications. A point of interest is that it uses the Ethernet and CBX LAN configurations together on the same LAN. The idea is to have a more responsive system by separating host traffic on the Ethernet and device traffic on the CBX. In terms of the generic base-line, the majority of devices connected via the Ethernet are considered to be host computers, and the majority of hardware accessing, or connected to, the LAN via the CBX will be considered to be devices (personal computers (PC), terminals, printers, etc.).

In reality, numerous combinations of microcomputers, mainframe computers, personal computers, peripherals (printers, disk drives, etc.), and terminals could be attached to the network. For the purpose of this thesis, it will be assumed that twisted pair, coaxial, or fiber optic cable could be used (in appropriate locations).

C. POSSIBLE USES/APPLICATIONS

An application is a "system" that has been defined to be suitable for implementation of electronic data processing techniques [Ref. 3: p. 22]. Common applications include word processing, data base management systems, spread sheets, and mail (message) systems. Specific applications can be developed and tailor-made for a user. Many applications can be purchased "off the shelf", while others are extremely complicated (space shuttle systems, navigation systems, C3 systems etc.).

For the generic baseline configuration this thesis will assume that all the common applications can be run, and that a high volume of mail traffic exists as a result of tailor-made applications. Two examples of high volume mail/message environments are C3 and large scale technical analysis operations.

D. ENVIRONMENTAL CONSIDERATIONS

"Computers have been shot, stabbed, stolen, and intentionally electrically shorted out." Environmental security once meant keeping a computer facility surrounded by locks, fences, guards, etc. Today's environment is much different with many small powerful computers, portable terminals, etc. Physical security concerns include controls that protect against natural disasters like fires, floods, or earthquakes; intruders or vandals; and environmental hazards like power fluctuations. Physical security controls are needed to regulate the environment surrounding the computer. Additionally, the environment includes areas not covered in this thesis: program libraries, logs, records, magnetic media, backup storage areas, and utility rooms. [Ref. 12: p. 21]

In sum, environmental security is more concerned with the physical ADP security arena. This thesis will be concerned more with security of the LAN configuration than actual physical device and building security. Nevertheless, there will be aspects of the configuration analysis that address certain physical threat areas (natural disaster, inadvertent actions, and deliberate actions). Consequently, an overview of considerations for physical access, electrical power, and the general environment will be presented.

Environmental factors follow with a brief explanation of threats or vulnerabilities, and general safeguards.

1) Physical building security -- vulnerable areas are adjacent to, within, above, and below any building containing an ADP center, ADP equipment, computer equipment room, media library, utility sources, and alarm systems, especially at periods other than normal work hours. Safeguards include [Ref. 19: pp. 2-3 FZ S-50]:

a) Building design: ADP center isolation; limited access routes; integrity of construction; reinforcement; underground communication/power lines; extensive lighting.

b) Physical barriers: fences; barred windows; locks; automated access systems; man-traps; secure storage containers (safes, etc.).

c) Guards and receptionists.

d) Electronic monitors -- includes intrusion detectors and object detectors.

e) Administrative procedures: access lists, sign-in logs, badges, etc.

f) Visitor control: authorization; inspection; records; etc.

2) Electric power -- basic threats are transients; brownouts; blackouts. Moreover, power surges can alter programs, erase memory, and destroy microcircuits. Possible safeguards include monitoring devices, spike suppressors, voltage regulators, dual feeds, and diesel generators. [Refs. 12,19]

3) Environment -- basic threats are temperature extremes, humidity, and particle contaminants. Safeguards include monitoring devices, redundant air conditioning, access to outside air for emergency ventilation, dust covers, bans on smoking. [Refs. 12,19]

4) Fire -- prevention includes building construction using fire resistant materials, and fire partitions and dampers where possible: ADP center isolation; periodic fire inspections; proper sprinkling systems. [Refs. 12,19]

5) Flooding -- threat sources include flood plains, water storage areas, water/steam pipes, and building leaks. Safeguards include building location and design, ADP center location, water seals, and drain systems. [Ref. 19: p. 6 FZ S-50]

6) Other considerations.

a) Neighboring threats: chemical or explosive operations, construction activities, airports, major roads, and high crime areas. [Ref. 19: p. 7 FZ S-50]

b) Electromagnetic interference include: elevators, cleaning equipment, power lines, radio and TV transmitters, microwave communications, and RADAR. [Ref. 19: p. 7 FZ S-50]

c) Communications failure: must provide adequate protection of communication links. [Ref. 19: pp. 1 S-27 Atch 13,1 S-28 Atch 4]

d) Computer hardware failure: prevention includes proper maintenance procedures and record keeping, security clearances for maintenance people, and contingency plans. [Refs. 12,19]

E. FUTURE EXPANSION

In general, there is a lot of flexibility and room for expansion in a LAN configuration because it can provide for the interconnection of a variety of data communication devices, an increased number of device nodes, and can be connected to other networks via gateways. To all that, more "applications" could be added, assuming appropriate hardware capability exists.

For instance, the generic configuration presented in this thesis could be expanded to provide standardized templates or "boiler-plates" for queries, menus, reports, data bases, RDT&E testing, DoD systems acquisition, etc.; generic data analysis; and project management. Also, expert systems could be implemented to assist with test and project planning. Thus, a LAN configuration is a natural tool to develop applications, prototypes, testing methodology, etc., via easy network interface allowing faster production and testing of configurations. This includes analysis of LAN computers, terminals, transmission media; and design of benchmark and LAN configurations.

Clear, too, is the possibility of internet network connection via gateways or bridges to wide-area networks. A single LAN configuration might be expanded to include multiple gateways to the same wide-area network, or several wide-area networks, via modification of existing device nodes and/or addition of gateways.

Given the generic LAN components and future expansion possibilities covered in this chapter, network management becomes more complicated when the network processes sensitive information. Security can be best applied early in the network design stages, but first a network manager needs to have a feel for the security guidance that applies to his or her network. The next chapter provides an overview of some existing security regulations and guidance and how it applies to LANs and networks in general.

III. SECURITY REGULATION AND GUIDANCE OVERVIEW

A. INTRODUCTION

Once any network (or ADP system) is required to process sensitive information, security measures must be implemented. In general, the degree of information sensitivity determines the extent of security control required for the system. Thus, the LAN configuration must be shaped to meet the security requirements for a given level of sensitivity.

1. Scope

a. What is Covered

In general, topics within selected regulation and guidance that pertain to ADP networks (i.e. LANs) are addressed along with limited risk management, physical and environmental aspects. Also, limited accreditation items relating to Army Regulation (AR) 380-380 ADP network accreditation requirements are addressed in this chapter. The accreditation process is discussed in more detail in Chapter V. Also, Chapter I may be referenced for an accreditation overview.

Regulation and guidance topics referenced by this thesis are placed in four broad categories:

1) Regulations and guidance that apply to LANs.
2) Regulation and guidance that DO NOT apply to LANs.
3) Outdated regulations and guidance, i.e. no longer applies
4) LAN areas and topics not covered by regulations etc.

All the categories are concerned with any ADP requirement that relates to networks as well as network specific requirements. Given the parts of the generic network description in Chapter II, applicability of guidance is based on general system-wide considerations and component level considerations. For example, a system-wide consideration is the sensitivity level(s) of information an entire system will handle. Thus, the corresponding sensitivity guidance is applied. Similarly, guidance for a remote mainframe computer terminal would be applied to network terminals (a network component). This approach is applied to all LAN component and "system-level" areas.

b. What is Not Covered

Personnel requirements are not covered by this thesis. Topics such as sensitivity of classified information that relate to personnel security are addressed.

2. Background

There is almost nothing in the guidance reviewed for this thesis that pertains to "LANs" specifically and very little in terms of direct references to "networks" in general. But, the guidance reviewed does address ADP security topics that relate to general LAN/network components. Remember, the thesis is restricted to existing guidance selected by USACDEC/DIM (guidance is listed in the following section of this chapter).

Because AR 380-380 is currently the focal guidance for ADP security in the Army, it is used as the origin for all other guidance reviewed for this thesis. Thus, the basic security topics covered in all regulations referenced are similar to AR 380-380: physical, environmental, personnel, communications, telecommunications, terminal access, hardware, software, procedural, risk management, etc. Yet to better summarize the limited number of network security topics, the AR 380-380 topics are combined into more general topic areas. These topic areas are sensitivity, physical/environmental, risk management, general communication (telecommunication, communications security, etc.), configuration (hardware, software, access), and general/miscellaneous ADP. Moreover, anything pertaining to a topic area is addressed in each of the four regulation categories mentioned above.

Before continuing, telecommunications, protected distribution system (PDS), communications security (COMSEC), and an automated telecommunications system (ATS) are defined. Telecommunications is the transmission, emission, or reception of signs, signals, writing, images, sounds, or other information over wire or broadcast medium to and from a distant location. A PDS, is an approved telecommunications system that permits safe transmission of unencrypted sensitive information by applying physical and electromagnetic safeguards. Note that the term "network" is not used [Ref. 13: p. 78]. Communications security is the protective measures exercised to deny unauthorized access to telecommunications information related to U.S. Government national security. Security measures include crypto-security, transmission security, emission security, and physical security. Cryptography is the art or science concerning the methods, means, and principles for making plain text unintelligible and for converting encrypted messages into intelligible form. [Ref. 13: pp. 72,73]

An ATS is a computer based system composed of terminal and/or automated switching equipment, interconnecting facilities, and/or control equipment, used for the purpose of transmission and reception of signals in the form of sounds, images, graphics, and data, and their associated firmware or software programs. Note that an ATS seems to equate to a general definition of a network in terms of device-to-device communication transmission. More on this is addressed in Category 4 comments below. [Ref. 13: p. 72]

B. GUIDANCE SUMMARIES

Guidance referenced for this thesis are listed below. A summary for each may be referenced in the Appendix.

- ARMY REGULATION 380-380: AUTOMATION SECURITY. Effective 8 MAR 86.
- ARMY REGULATION 380-5: Deptartment of the Army Information Security Program. Effective 15 FEB 85.
- ARMY REGULATION 18-1: Army Automation Management. Effective 15 SEP 80.
- TECHNICAL BULLETIN TB 18-100: Army Automation Life Cycle Management. Effective 15 AUG 81.
- ARMY PAMPHLET 18-4: Processing Installation Review/Evaluation Checklist. Effective 1 SEP 85.
- ARMY PAMPHLET 18-7: Automatic Data Processing Management Review Guide. Effective 3 DEC 85.
- ARMY REGULATION 530-2: Communications Security (COMSEC) Effective 1 SEP 82.
- ARMY REGULATION 18-7: Automatic Data Processing Management Review Program. Effective 30 NOV 84.
- ARMY TECHNICAL BULLETIN TB 18-107: Army Automation Automatic Data Processing Equipment Operations Management. Effective 3 FEB 86.
- ARMY REGULATION 380-53: Communications Security Monitoring. Effective 15 NOV 84.
- DEPARTMENT OF DEFENSE (DoD) MANUAL DoD 5220.22-M: Industrial Security Manual for Safeguarding Classified Information. Effective 1 MAR 84.
- DoD DIRECTIVE 5215.1 (DoD Directive 5215.1), SUBJECT: Computer Security Evaluation Center. Dated 25 OCT 82.
- DoD MANUAL 5200.28-M: ADP Security Manual Techniques and Procedures for Implementing, Deactivation, Testing, and Evaluating Secure Resource-Sharing ADP Systems. Dated JAN 73.
- DoD COMPUTER SECURITY CENTER CSC-STD-001-83: DoD Trusted Computer System Evaluation Criteria. Also known as the "ORANGE BOOK". Dated 15 AUG 83.
- DoD DIRECTIVE 5200.28: Security Requirements for Automatic Data Processing (ADP) Systems. Dated 18 AUG 72.

- NATIONAL COMPUTER SECURITY CENTER PUBLICATION NCSC-WA-002-85: Personal Computer Security Considerations. Dated 1985.

C. CATEGORY 1: GUIDANCE/REGULATIONS THAT APPLY TO LANS

Since information/data sensitivity determines the security requirements for the ADP system that handles it, sensitivity requirements and modes of operation will be addressed first. To emphasize the limited number of direct references to networks, general network guidance references will be addressed next, then other general ADP topics that pertain to networks will be presented. Since there are so few direct references to "LANs" and "networks" in general, the rest of the thesis will use the two terms interchangeably.

1. Sensitivity

All guidance references stressed that sensitivity of data be based on an individual's need-to-know the information in relation to performance of duty. The need-to-know must be a valid, approved need, based on the information contained in the system and the information's potential damage to national security, if it was some how leaked or stolen. [Ref. 20: p. 10] Sensitivity designations are divided into broad categories with the flexibility for an accreditation authority to impose more restrictive designations. The accreditation authority is the official designated to accredit DPAs and ATSs for the processing, production, use, and storage of sensitive defense material [Ref. 13: p. 71].

Sensitivity applies to ATS, administrative, and normal ADP systems, therefore this thesis will assume it must apply to LANs as well [Ref. 13] Moreover, in terms of need-to-know, basic ADP sensitivity requirements are similar for contractor access of most types of classified information. In short, security requirements for components (transmission media, terminals, controlling devices, etc.) result from the assigned sensitivity level.

AR 380-380 sensitivity designations are divided into four levels just as the designations in the Department of Defense Trusted Computer System Evaluation Criteria (CSC-STD-001-83), also known as the "Orange Book". The thesis will refer to it as the Orange Book from this point on. The sensitivity requirements in each document are similar, but labeled different. Reference the Appendix summary of the Orange Book for a label comparison. We will use the AR 380-380 designations listed below. [Refs. 13,21: pp. 6,5-51]

- **CRITICALLY SENSITIVE (CS).**
  - **Applies to DPAs/ATSs that process classified defense information or applications involving large dollar volume assets, and resource accounting or authorization data greater than $25 million per year.**
  - **Levels in descending order of sensitivity. a) Level 1 (CS1) - sensitive compartmented information (SCI) or Single Integrated Operational Plan--Extremely Sensitive Information (SIOP-ESI). b) Level 2 (CS2) - TOP SECRET. c) Level 3 (CS3) - "SECRET/CONFIDENTIAL information or applications involving large dollar volume assets or resource accounting or authorization data ($25 million per annum or higher)." Large dollar volume assets and resources refer to items that range from weapons (like tanks) to large stock piles of supplies, for example millions of dollars worth of telephone poles stored in one location.**
- **HIGHLY SENSITIVE (HS) applies to:**
  - **DPAs/ATSs not included in "CS" above, that process FOR OFFICIAL USE ONLY (FOUO) information.**
  - **Information covered by The Privacy Act of 1974.**
  - **"Asset or resource accounting of authorization data of dollar value greater than $1,000,000."**
  - **Any unclassified data the accreditation authority wants to classify at this level.**
- **SENSITIVE.**
  - **Applies to information not covered by "CS" or "HS": a) DPAs/ATSs that "process information relating to asset or resource, proprietary or contractual information". b) Any data the accreditation authority wants to classify at this level.**
  - **"Includes data vulnerable to fraud, theft, misuse, misrepresentation, or interception."**
- **NONSENSITIVE.**
  - **An analysis has indicated that a higher classification is not required.**
  - **Analysis must be approved by the installation system security manager (SSM).**
  - **Analysis must be kept on file and reviewed.**

Sometimes a higher classification may be assigned to combinations of information which warrant higher classification than that of the single parts of information. This is known as "compilation". This includes combinations of certain types of data/information (defense plans, technical information, etc.), and large dollar volume asset or resource accounting amounts. [Ref. 20: p. 11]

2. ADP Security Operation Modes

Possible operation modes for the above sensitivity levels require certain non-waiveable features (passwords, audit trails, etc.) [Ref. 13: p. 8] The operation modes that apply to all types of systems (ADP, ATS, etc.) are listed below. [Ref. 13]

- MULTILEVEL SECURITY MODE.
  - A trusted system of operating system software, hardware, and firmware.
  - Restrictions. a) Need written approval of ACSI to use multilevel. b) If intend to secure accreditation, must notify ACSI prior to milestone 0.
  - All CS1 or CS2 systems need the specific written approval of the ACSI.
  - This mode does not apply to CS3 and lower sensitivity systems.
- CONTROLLED SECURITY MODE.
  - Characteristics [Ref. 13: pp. 7-8]. a) Untrusted operating system software. b) System secure for highest information security level. c) System accesses no more than two security clearance levels below the highest level of information on the system. d) Each terminal area can be secured for the highest level of information processed through the terminal located in that area, i.e. semi-multilevel because different terminal areas may have different access levels.
  - Controlled security mode requirements apply from host to all remote locations. Again regulation is in terms of general ADP networks, not LANs. [Ref. 13: p. 42]
- SYSTEM HIGH MODE.
  - "The central computer system and all of its connected peripheral devices and remote terminals are protected according to the highest classification of material in the system."
  - All personnel accessing the system have a security clearance, but not a need-to-know all material in the system.
- DEDICATED SECURITY MODE [Ref. 13: p. 8].
  - When a computer system (terminals, peripherals, etc.) is classified for a certain type/category of information, and all users have the same security clearance and the need-to-know.
  - Required for all systems unless one of the above modes is approved by the accreditation authority.
- PERIODS PROCESSING [Ref. 13: pp. 8,46]
  - "Included in the Dedicated Security Mode when the entire system is used for a specific period of time for a category, type, or classification of information."
  - People must have the appropriate security level for the time(s) they access the system.
  - Can be used for certain types of information on systems accredited in the systems high and controlled security modes.

3. General Network References

a. General Direct References

Even though there are few references to "networks" in AR 380-380, it defines "networks" as one of several operational service modes, and the most vulnerable [Ref. 13: p. 7]. At best, AR 380-380 mentions network specific positions: network manager, network security officer, and a terminal area security officer (TASO) for remote terminals which are network related. Moreover, one manual addresses all aspects of ADP (remote devices, telecommunications, etc.), but does not mention "network" except in ADP and communications networks interfaces. It states that security measures must meet telecommunications network requirements and be cost effective. [Ref. 22]

Furthermore, the only direct literal reference in one Army regulation is to the Defense Data Network [Ref. 23]. Other guidance referenced contained some "network" checklists [Ref. 24], and noted that they are only a "checklist" [Ref. 25]. Another directive pointed out that the Computer Security Evaluation Center (CSEC) purpose includes evaluation of "network security." This indicates that government regulators are concerned with network security and not just security of specific ADP component categories, but still networks are not addressed as an entity in great detail [Ref. 26]. The guidance documents referenced for this thesis should at least reference some form of LAN/network guidance, or at least identify important LAN/network topics within.

b. General Indirect References

As mentioned earlier, most of the guidance addresses general ADP system components that are often part of networks, as well as stand alone computer systems. By addressing these ADP parts, or components, overall network security considerations can be obtained. As a result, the network accreditation authority must ensure that the network component security requirements produce a synergistic effect that yields the desired level of system security for the network. This idea applies to direct and indirect guidance requirements identified throughout this thesis.

4. Risk Management

Risk management is defined by AR 380-380 as "an element of managerial science concerned with the identification, measurement, control, and minimization of uncertain events." Procedures are not standardized because every system is unique. There are four phases [Ref. 13: pp. 29,77]

- Risk assessment derived from an evaluation of vulnerabilities and threats.
- Management decision.
- Control implementation.
- Effectiveness review.

Vulnerabilities and penetration are addressed by this thesis in general ADP terms. [Ref. 13: pp. 67-69]

Again, as mentioned in Chapter I, a risk management analysis is assumed to be complete for the generic LAN presented in Chapter II. A risk management analysis is an important, but lengthy process in terms of this thesis. It should be conducted in a real-world implementation because it is intended to assist with the network sensitivity designation. In order to limit the scope of the thesis, it is assumed that a adequate risk management analysis was conducted that identified all vulnerabilities (this is an ideal situation).

5. Configuration Control

Configuration control regulations and guidance are presented in access, hardware, and software topic categories. Again, material presented here is a general summary of ADP components and processes that apply to network components.

a. Configuration access control

Access security for an ADP system is concerned with control of procedures, information, access to terminals/devices, and resource sharing. AR 380-380 and other guidance is based on a need-to-know with "access" only to the hardware devices and software needed to accomplish an assigned task. The general idea of security access control procedures is to minimize vulnerability during authorized and unauthorized start up and shut downs, provide mandatory control of ATS jobs on all new Army systems, and provide transaction logs for accountability. [Ref. 13: pp. 24-25]

In general, actual information access control to data files is based on mandatory access control and discretionary access control. Mandatory access control is

> a means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e., clearance) of subjects to access information of such sensitivity.

Discretionary access control is

> a means of restricting access to objects based on the identify of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject. [Ref. 21: pp. 110,111]

By consequence, pure data control requires an auditable record of data as that data is processed through the system. In fact, this is one of the few places where "network" is mentioned literally. [Ref. 27: p. 2-1]

Before an ADP system, terminal or device, or a network can access or interface to a specific ADP network, the ADP system, device, etc., must meet approval of the DoD component, and the agency operating the net. Normally, the agency and component have responsibility for security of a network [Ref. 22: p. 20]. In addition, sharing of ADP resources between agencies needs approval. The guidance addresses resource sharing in an ADP context, but can be easily applied to networks. For instance, an administrative LAN typically requires sharing of peripherals for word processing, data base, and other applications. [Ref. 27: p. 7-1]

b. Hardware and Software

Most hardware configuration control guidance is in terms of a single ADP configuration with a central mainframe site. Life cycle security planning is required from beginning to end and applies to networks, nodes, and terminals as well as general ADP systems. [Ref. 13: p. 10].

Acquisition of entire ADP systems or components is a function of mission need. To streamline acquisition and give it flexibility, AR 18-1 encourages low level decision making (to "practical levels"), and stresses ADP decentralized management concepts. If the reader is currently involved, or about to begin, some sort of ADP network security planning or implementation, he/she may find that general integration and streamlining of regulatory ADP network guidance may also be a desired tool for system acquisition. This thesis could be used as a primer for such a project. Decentralized management seems to be a good environment for LANs because of their distributed yet inherently unsecure nature. In addition, AR 18-1 states that Army ADP management principles must comply with federal laws and regulations. [Ref. 28: pp. 1-1,1-2,2-1]

In terms of network hardware and software components, some guidance (such as AR 380-380 and Army Pamphlet 18-7) provide checklists. Checklists include configuration optimization, communication, emanation, and remote access security. Checklists in Army Pamphlet 18-7 must be completed on an annual basis, when there are equipment upgrades, or major agency reorganization. [Refs. 13,24]

Another point of interest is that personal computers (PCs) must be accredited with a specific ADP system if the PC will interconnect, or be collocated, with that system more than 50 percent of the time. The same security requirements (in relation to need-to-know, etc.) that apply to the ADP system apply to the PC(s). In addition, a privately owned PC can only be used in a stand alone configuration, but must comply with all provisions of AR 380-380 and other guidance. Information processed becomes the property of the agency in which it is used. [Ref. 13: pp. 9-10]

It is required that "software-based protective controls complement and support hardware protective features of computer circuitry." General purpose software categories (executive, utility, tools for development of applications software, and applications software) all require adequate software security controls. Again, security requirements must be appropriate for the sensitivity level of the system. Guidance on operating systems is addressed in Chapter IV. [Ref. 13: pp. 20-22]

6. Physical/Environmental Considerations

Physical and environmental guidance requires physical facility access controls that meet security and protection standards appropriate for the sensitivity levels of information handled by any ADP system. This includes ADP administrative and network systems. Even though personnel security is not addressed directly in this thesis, it does play a major role in all aspects of ADP security. One point stressed by AR 380-380, and other guidance, is that protection of remote terminals/sites requires they be staffed with people cleared for the highest security classification level cleared for that particular site. For example, this is a requirement of the controlled security mode. [Ref. 13: pp. 21,45]

7. General Communications

ADP-to-ADP equipment communication links can be intersystem, internetwork, and intranetwork. With so many possible device-to-device interfaces, standardization of ADP component connections is a major Army ADP management goal. Naturally with or without standardization, connection of ADP systems or networks require awareness of security requirements of the other system and agency. [Refs. 13,28,29]

Army COMSEC policy requires that all record telecommunications will be secured by either PDSs or encryption in approved cryptographic systems. In addition, guidance indicates that PDSs have physical and electromagnetic safeguards approved on a case-by-case basis. The PDS must be approved for a certain sensitivity level and mode of operation [Refs. 13,29: pp. 76,10]. Moreover, all circuits that interconnect remotely located components of Army automation systems or networks must be provided COMSEC protection under the provision of AR 530-2. COMSEC can be achieved by proper implementation of:

- National Security Agency (NSA) produced cryptographic systems.
- An approved Protected Distribution System (PDS).

- Approved commercial communications protection equipment. [Ref. 13: pp. 18,44]

In contrast to encryption and other requirements, guidance recognizes that enemy technical developments could render current encryption processes and components useless. Thus, continuous evaluation of communication links for encryption and system emanation vulnerabilities, and emergency procedures, should be part of system operations wherever remote ADP components exist. [Ref. 29: pp. 2-3] Vulnerability and hearability (emanation detection) surveys may be requested for ADP systems to test susceptibility of communication signals to monitoring. These tests determine the degree of security of system cryptography. Cryptography applies to TOP SECRET, SECRET and CONFIDENTIAL system processing. [Ref. 30: pp. 4-5]

D. CATEGORY 2: GUIDANCE/REGULATIONS THAT DO NOT APPLY TO LANS

Given the fact that there are few direct literal references to network security in the guidance referenced, the topics covered in this category will address general network related ADP guidance topics in terms of sensitivity, communications, and configuration control. Moreover, each of these areas will be separated into waivers and exceptions. An exception is a case to which a rule does not apply. A waiver is "the act of intentionally relinquishing or abandoning a known right, claim, or privilege." Additionally, this thesis will assume a waiver is equal to a "temporary exception." [Ref. 31: pp. 432,1325]

1. Sensitivity

Sensitivity waivers deal mainly with time limits and/or extensions.

a. Waviers

In reference to security operating modes general ADP guidance (like AR 380-380) recognizes the need for temporary exceptions with intent to obtain full security compliance. Moreover,

> temporary exceptions may be authorized by the. . . Designated Approving Authority. . . for specific security measures which they have determined would impair operation and mission effectiveness, provided they assure that continuous progress is made toward the ultimate full compliance with the Directive at the earliest practicable time.

Also, the approving authority should not delegate authorization authority. [Refs. 13,32: pp. 9,5]

b. Exceptions

In AR 380-380 the MACOM-commander or heads-of-Army-elements may direct higher sensitivity levels. Conversly, for CS2 systems: "the accrediting authority may designate the DPA at one level of sensitivity lower than that prescribed. . . if all the following conditions exist".

- "The volume of information in the higher level of sensitivity requires less than 5 percent of total processing (wall clock) time."
- Higher level sensitivity information is processed in the local operational service mode (AR 380-380 paragraph 1-11b(1)) and Dedicated Security Mode (paragraph 1-13d).
- "Additional security and protective measures are taken to safeguard the information of the higher level of sensitivity."
- "All personnel have the security clearances for the highest level of classified information to which they may be exposed. (AR 380-5 applies)." [Ref. 13: p. 6]

The higher the sensitivity level, the higher the approval authority required to approve an exception. For instance, in the multilevel security mode, exceptions are "prohibited for all CS1 or CS2 systems without the specific written approval of the ACSI"; and but this is not applicable to CS3 and lower sensitivity systems. [Ref. 13: pp. 7-8]

In general, exceptions must be reviewed biennially and specific security requirements may have to be interpreted when applying security level criteria. [Refs. 21,32: pp. v,5]

2. General Communications

Exceptions to transmission requirements must offer the same degree of protection as approved components, processes and procedures. If less protection is provided it may be possible to go to the next higher approval level. Exceptions will depend on characteristics unique to the system, which may include the sensitivity of the information, the characteristics of approved ADP equipment, the characteristics of substituted equipment, the results of a risk analysis, and the organizations involved. In addition, exceptions for ADP systems becoming part of a network must be addressed before actual connection. [Refs. 13,32,20]

3. Configuration Control

a. Waivers

General ADP security waivers are listed below [Ref. 13: p. 9].

- "Accreditation authorities may grant waivers or exceptions to existing systems when compliance with this regulation is not technically, economically or operationally feasible. However, all changes, updates, and procurements will have as an objective elimination of waivers or exceptions."

- "The condition or situation for which the waiver or exception is requested will be described and the justification given in order for the request to be evaluated."
- "Waivers or exceptions will be limited to a specific period of time, not to exceed 1 year. Exceptions or waivers will not be renewed or extended without the written approval of the accreditation authority. This extension will detail specific actions taken to correct the situation or circumstances necessitating the extension."
- "Waivers will be included in the Executive Summary portion of the accreditation documentation." Reference Appendix I in AR 380-380.

b. Exceptions

Discretion should be used in applying security provisions to automated administrative systems because not all of the guidance requirements are applicable to them. However, "the provisions of Chapter 5 (of AR 380-380) are applicable to all systems processing classified information." [Ref. 13: pp. 2-10]

E. CATEGORY 3: OUTDATED REGULATIONS AND GUIDANCE

Guidance addressed by this thesis is the most current available at the time of writing. Guidance topics addressed in this category are not considered "outdated" in the literal sense because usually the most recently dated regulation, directive, etc., is in force until a revised version is produced. Certain aspects of the guidance referenced give the impression that some requirements are outdated or perhaps "old fashioned" in the world of developing ADP technology. For instance, administrative (word processing, etc.) and general ADP configurations seem to be addressed in terms of the old mainframe type of configuration, which does apply in a true ADP mainframe environment, but ignores a distributed network environment [Ref. 13: pp. 9-10]. From all information, AR 380-380 seems to give the impression that a central site always exists as a "main" site. With the above points in mind, and, as pointed out earlier, the fact that networks are not specifically addressed in great detail as an entity, topics in this category are subjective. [Ref. 13]

Some of the guidance referenced recognizes that it's objectives could adversely affect use of rapidly changing technology. In fact, guidance as early as 1973 (DoD Manual 5200.28-M) states "this technology is dynamic and the methods chosen to secure a particular system must accommodate new developments without degrading the level of protection." The same manual notes that new technology or security substitutes must be cost effective, production effective, and meet basic security levels. [Ref. 22: p. 2]

Points of interest in this category relate to physical/environmental and configuration control topics.

1. **Physical/Environmental**

In reference to the above points, much more attention is directed toward the "central site" verses a true distributed network. For example, the construction of a "central" computer complex and the "mainframe" computer room is addressed. This definitely applies to mainframes, which still exist and will for many years to come. In terms of networks and recent increases in desktop capacity and capability, more specific guidance should be developed and integrated into, or added to, current guidance [Ref. 13: pp. 12-16]. Thus, guidance in this area still applies to mainframe configurations, but is not totally complete in terms of networks and PCs.

2. **Configuration Control**

a. Software considerations

There are references to configurations that involve over the counter batch applications (very common in the 1960's). References also address media handling requirements that still include requirements for punch card decks. Is the operational age range of Army equipment so vast that modern punch card applications still exist in significant numbers? Or, has the acquisition process slowed replacement of such systems? Whatever the reason, a general indication is that "new" technology strategies and applications need to be added to Army guidance. [Refs. 13,20]

b. Stand-Alone PC Duplication

AR 380-380 states that stand alone systems should not duplicate standard Army systems. Again, AR 380-380 seems to ignore distributed processing and desktop capacity. There may be (or are) standard Army systems that could be transferred to desktop computers to provide emergency processing, backup processing, increased capacity or production, or any other unique innovated tests or processing that can be devised to improve productivity. [Ref. 28: p. 2-2]

c. Summary

Some areas of the guidance appear to be outdated in terms of today's desktop and distributed processing capability. Also, there is a mainframe flavor in the guidance and even reference to punch card requirements. In essence, the guidance covered in this section is outdated because it does not address considerations for distributed computing protection and security of PCs.

F. CATEGORY 4: LAN AREAS AND TOPICS NOT COVERED BY GUIDANCE

1. Overview

Again, the majority of the security guidance mentions network related components, not network specific topics. Thus, much is left to interpretation in terms of LAN/network security in areas not covered by the guidance.

2. ATSs vs. ADP Networks (i.e. LANs)

Chapter 11 in AR 380-380 is devoted to ATSs. Above, it was assumed that an ATS is very much like a network. The regulation implies that a network consists of two or more automated systems [Ref. 13: p. 5], but hardly mention ADP networks as an entity. Is it a question of semantics? Given there are network check lists (mentioned above) and other limited references to networks, it is assumed that an ATS is at best a hybrid ADP network or an ADP network is a hybrid ATS. As mentioned at the beginning of the chapter, an ATS closely parallels the definition of a general purpose network. In today's rapidly changing technical environment is it safe to assume an ATS has the exact same needs as an ADP network? If so, why is it not at least stated that a network equates to an ATS? Again, an ADP network is not addressed literally and topically as an entity.

3. Configuration Components

Again, nothing specific is mentioned about network component combinations. Only general ADP components are addressed.

4. Software

The only thing mentioned in specific network terms is that the network security officer (NSO) is to ensure that protocols are developed for networks. Specific network protocol guidance is not referenced. The software categories identified are general purpose; executive; utility; and software tools for development of applications software. Protocols would probably fall under the utility program category. A utility is "a program provided by a computer center or vendor to perform a task that is required by many of the programs using the system." Because "utilities" is a general category, a protocol could be thought of as a communication or interface utility. [Ref. 13: pp. 20-22,389]

5. Network Audit Procedures

Again networks are not specifically mentioned in AR 380-380, but it does specify mandatory audit trails for all new teleprocessing systems. [Ref. 13: p. 24]

6. Peripherals vs. System Approach

a. Accreditation

A device must be accredited with a system if it is connected to the ADP system more than 50 percent of the time [Ref. 13: p. 9]. Network configurations can have many personal computers that do not need to access the network 50 percent of the time. With current desktop capability, a desk top could make it's presence noticed in terms of network capacity and throughput. In addition, a hacker/spy could do real damage to a network with a PC. Is this impact of PCs really addressed? Not directly in terms of the guidance referenced for this thesis. This is another area that could be updated and made more network specific.

b. PC security

Issues related to networks are penetration and access. "Personal Computer Security Considerations" NCSC-WA-002-85, published by the National Computer Security Center, covers PC security issues, an area not thoroughly mentioned in terms of todays network technology in the guidance addressed in this thesis. This document is NOT government policy, but an information memorandum. It addresses PC penetration, communication access, and transmission to networks, and other general information. [Ref. 33]

G. THE NEXT STEP

This chapter indicated that even recent ADP security guidance (1986) does not mention LANs, but must be used to shape LAN security features. Given the preceding overview of security guidance, the next step is to take a closer look at security guidance for the system hardware, software, and transmission components found in a LAN.

IV. BASIC NETWORK SECURITY DEVELOPMENT CONSIDERATIONS PERTAINING TO COMPONENT GUIDANCE REQUIREMENTS

A. PART 1: OVERVIEW

As indicated in the previous chapter, a "need-to-know" is the driving force behind sensitivity levels and the ultimate classification of any ADP system, including LANs. Guidance indicates that the need-to-know in the pure sense is a major consideration for determining a sensitivity level. Whether the need-to-know is really the driving factor in every network now, or in the future, or how it is determined, is not within the scope of this thesis. However, a sensitivity level must be assigned, thus we will assume a valid need-to-know can be determined, and look further at sensitivity considerations.

Chapter III looked at guidance areas that applied and did not apply to LANs. In contrast, Chapter IV looks at the same guidance in terms of how it applies to various LAN components, and the LAN configuration as a whole. From all information, the accreditation authority will have the ultimate approval, and at least share responsibility, in terms of what actually applies because each system is unique. Chapter V addresses accreditation.

This chapter is divided into four parts. The overview (Part 1) explains component categories and a basic regulation planning strategy. Part 2 presents general guidance requirements for networks derived from the ADP and telecommunication guidance referenced for this thesis. Part 3 and 4 review general network requirements pertaining to multilevel and system high (respectively) security modes. Note that all material in this chapter is based on the regulations covered in Chapter 3.

1. Chapter IV Component Categories

Chapter II is structured around functional network categories like topology, protocols, internetworking, etc. For better identification of component topics, LAN components in this chapter are listed in terms of general ADP topics presented in the guidance. The major categories are general system considerations, ADP hardware, transmission hardware, and software. The categories and components are listed below.

- SYSTEM/MISCELLANEOUS CONSIDERATIONS
  - Configuration
  - Sensitivity
  - Mode

  - Procedures
- HARDWARE - Computers
  - Mainframes
  - Minicomputers
  - Microcomputers
- HARDWARE - Interface
  - Controler Devices
  - Switches (CBX/PBX)
  - Protocols (hardware aspects)
  - Bridges
  - Gateways
  - Modems
  - Multiplexers
- HARDWARE - Terminal devices
  - Smart terminals
  - Computer terminals
  - Microcomputers
  - PCs
  - Printers
  - Electronic Storage (disk, tape, etc.)
- TRANSMISSION MEDIA
  - Twisted pair
  - Coaxial
  - Fiber optic
- SOFTWARE
  - Application
  - Interface (Protocols like Ethernet)
  - Operating system (general functions)

2. A Strategy for Applying General ADP Guidance to a Network

Strategy is defined as a "careful plan or method." [Ref. 31: p. 1165] Understandably, system designers and accreditation authorities must be careful in the way each unique system is analyzed with regard to guidance requirements, because security guidance is not and cannot be hardware and configuration specific. Thus, given an application and configuration, the strategy listed below is also in general terms.

1) Determine sensitivity range of information.

2) Identify tentative operation mode alternatives.

3) Place components in appropriate category; includes identification of performance capabilities.

4) Identify general system level requirements relating to categories.

5) Identify general component requirements relating to categories.

6) Identify operation mode requirements for each mode selected (multilevel, system high, dedicated, etc.)

7) Re-evaluate operation mode alternatives and select; based on each organization's unique requirements.

This chapter covers steps four, five, and six. Steps one, two, three, and seven are user, organization, and vendor/system specific and must be performed by the organization planning to implement the LAN. In reality, step three would be done in terms of specific components with consideration of associated specifications. The component guidance categories above would be used to isolate guidance that pertains to each particular component and system level consideration. Steps four, five, and six are illustrated in this chapter in a general way to point out guidance areas important to LAN security. Only two modes are chosen for brevity.

B. PART 2: GENERAL LAN - GUIDANCE REQUIREMENTS FOR NET WORK COMPONENTS

1. System/Miscellaneous

a. Configuration (Includes Topology)

LAN system configuration requirements are concerned with design, operation (coordination and control), facility, and hardware considerations. Guidance addressed by this thesis does not address LAN security in great detail. Various telecommunications, ADP, and ATS components are all used to establish LANs. These component requirements are addressed in enough detail to be applied to the ADP and transmission hardware used in LAN configurations. Guidance for LAN system level requirements can also be derived, just as ADP and telecommunications guidance can be derived and applied to LAN components.

The derivation idea in the above paragraph can be seen in the regulations themselves. For instance, ATSs and administrative systems are the only unique systems addressed in contrast to miscellaneous network comments. Configuration areas not covered under ATS guidance, are subject to general ADP requirements. In addition, administrative systems are not affected by security guidance unless they handle sensitive information or communicate with other computers. Thus any LAN is subject to ATS and general ADP requirements, even if it is purely an administrative system, because LANs consist of ADP components and always include telecommunications. [Ref. 13: pp. 9,31]

Keep in mind that the "system", or total configuration, must be approved. It is the responsibility of the organization commander or manager to see that AR 380-380 is applied [Ref. 13: p. 12]. The temporary exceptions and waivers addressed in Chapter III should be addressed as early as possible. The approval process, referred to as accreditation, will be addressed in Chapter V.

(1) *Design.* System security features should be incorporated into any LAN configuration from the very beginning. Minimum ADP system security requirement features that should be part of a LAN design include:

- Individual accountability - who is accessing and what they are doing
- Environmental control - physical protection of hardware.
- System stability - all components protected to provide steady operation.
- Data integrity - accurate and timely data.
- System reliability - minimize down time caused by security breaches and identify/prevent unauthorized penetration.
- Secure communication links - identify/prevent unauthorized penetration.

These features should also be applied to future upgrades and/or expansion. Standardization should be incorporated where possible with the ultimate goal of interoperability. Performance measures must allow for security needs because overall system performance may be affected by security software or hardware. Some examples involving encryption and shielding are presented later. [Refs. 13,32,34]

If system security features are to be included early in the design process, they should be followed throughout the system life cycle. For instance, any communication need should include security requirements whenever there is some sort of change or upgrade because new equipment could impact the total security of the current "system". For example, the use of fiber optic cable media could reduce the need for encryption. Thus, all applicable security requirements should be followed for all components of the system. [Refs. 13,17,28]

Emanation is the radiation of signals from a transmission cable media, hence it is another major system security design area to cause concern. Generally, the guidance sources indicate that some form of encryption is desired for sensitivity levels starting at CONFIDENTIAL and above. [Ref. 20: pp. 36-37] Encryption is the transformation of information into a unidentifiable code. In order to conform to compromising emanations control policies, the overall network system design will include link encrpytion or end-to-end encryption, and manual procedures for encryption key control. Either form of encryption will require extra hardware for key generation and encoding at the node interface to the network. Manual procedures must be used to control storage, issue, and control of encryption key information. All key information and handling procedures, encryption hardware and facilities, and software and associated storage facilities, must be protected at least at the highest security level for the system. Additionally, investigations and studies of compromising these emanations is given the unclassified name of "TEMPEST" [Ref. 13: pp. 5,78].

All transmission media and interface hardware will achieve security via one of the COMSEC methods; National Security Agency (NSA) produced cryptographic system, protected distribution system (PDS), or commercial communications protection (for unclassified national security information). A PDS is an approved telecommunications system that has the required physical and electronic safeguards for safe transmission of unencrypted sensitive information [Ref. 13: p. 76] These methods are to be used for all transmission hardware interfaces and are addressed in more detail under the transmission hardware section of this chapter. [Ref. 13: p. 18]

System planning should not isolate physical and environmental security considerations from other system security considerations. Topics like sturdy building construction, adequate electrical power, well constructed cable media supports, and proper routing and shielding of cable must be considered. The goal is to protect the system from unauthorized access and physical damage. [Refs. 13,23]

Finally, future system improvements must be state-of-the-art, not duplicative, and cost effective, as well as approved by the accreditation authority. To accomplish this, the design should be modular to the extent that additional connections are possible for extra security hardware and software features that may be required. Security upgrades and/or additions of existing security features should not degrade overall system performance. [Ref. 13: p. 9]

(2) *Operations - Coordination and Control.* System interoperational security considerations concern intra-system as well as inter-system activities. LAN configuration control must be rigid, well established and enforced. In addition, a

comparison between the baseline configuration and a proposed modification must be made before any system component is modified. The comparison must include a system security evaluation that includes audits of hardware, software, and firmware, and risk assessment. Also, auditors should be involved in all phases of the design process to assure that audit trails are properly designed and integrated into the network. [Ref. 13: p. 32]

Security coordination within a LAN should be between the ADP network security officer (ADPSSO), terminal area security officer (TASO), network security officer (NSO), and the network manager. In contrast to standard mainframe terminals, the TASO may not only be responsible for "terminals" at his/her remote location, but gateway hardware, mircocomputers, or network control hardware (switches, controllers, etc.). In terms of a network, the ADPSSO would be responsible for security of one or more computers at a particular site. Yet he/she would be subordinate to the NSO because their site is a remote user of the network just as a terminal is a remote user. Therefore, a NSO may manage many TASOs and ADPSSOs. ADPSSOs may have their own TASOs for their local equipment. Also, security at the internet level could be handled by the network manager or NSO. [Ref. 13: pp. 4-5]

Special attention should be paid to requirements of organizations that maintain telecommunications networks, especially to the transmission interface gateways. This includes requirements for data link interfaces, message link interfaces, and encryption requirements. Data link security is in terms of pure bit stream transmission. Message link security deals with actual encryption of the message handled by the protocol. [Refs. 35,23: p. 7]

Network configurations are the most vulnerable ADP operation mode because of their on-line, interactive, and distributed nature [Ref. 13: p. 7]. Thus, continuous safeguards are a must. In essence, networks are systems composed of ADP hardware components, software components, and transmission media components working together. Similarly software security, hardware security, procedural security, physical and environmental security, and communications security must work together to provide efficient network "system" security.

In terms of system operations security, the NSO must compile a security profile that describes equipment components, equipment locations and relationships, the physical structure, and general operating environment of the automated system. This is especially important in a PDS without encryption, because physical protection and electronic shielding could be penetrated at almost any physical point of the network. [Refs. 13,23: pp. 76,6]

(3) *Facilities.* General environmental protection must include cost effective detection, protection systems, and emergency measures to provide disaster (fire, flood, etc.) protection. The goal is to minimize system and information vulnerability that would result from a disaster. Thus, network facilities must be properly designed and constructed. [Ref. 13: pp. 10-12]

In stand-alone ADP networks the central facility is usually the room/building that contains the computer. In a network it is any location that contains the network control components. Given a network can have distributed control, all network facilities housing network control components and gateways should be protected according to ADP "central facility" requirements. The central facility must always equal the requirements for the highest approved system security classification, especially if it is a contractor operated system or a system under contractor development and implementation. [Ref. 36: pp. 177-178]

(4) *Hardware.* Hardware security requirements for ADP equipment apply to all LAN ADP hardware and LAN interface devices; controllers, gateways, and computers controlling protocols. These requirements must be considered in all future Army systems. Hardware features required in terms of the "system" configuration are internal isolation of users, user port and/or channel identification, internal protection mechanisms for memory and storage, and error detection. External security features include facility security and physical locking devices such as insertion of keys or magnetically encoded cards. [Ref. 13: pp. 19-20]

b. Sensitivity - Levels and Applicability

System sensitivity must be determined before a secure operating mode can be designated. In addition, a risk management program must implement procedures to identify weaknesses so effective counter measures can be devised.

(1) *Sensitivity determination.* In sum, requirements identified in Chapter III (of the thesis) indicate that sensitivity is determined by the importance of the information processed to the overall Army mission, a need-to-know, and unique system features or applications that warrant protection.

Sensitive data includes personal data protected by the Privacy Act of 1974. In short, personal data of all personnel maintained on any ADP system is considered "highly sensitive" information in terms of the sensitivity categories preseented in Chapter III. [Ref. 13: p. 6]

In addition to Privacy Act data processing, sensitivity is determined by the user, dollar value, and/or value in terms of national interest or defense. A need-to-know applies to all aspects of the system configuration. Also, a system Accreditation Authority can impose more rigid sensitivity levels for reasons unique to a particular system. [Ref. 13: pp. 6-7]

Sensitivity requirements identified in Chapter III also indicated that "compilation" of unclassifed items may require a higher classification. This requires system unique analysis to determine if in fact a sensitive compilation of information exists. Because of network distributed processing and access, compilation is always a consideration in a network. Given the system analysis, the original classification approval authority makes the final classification determination, but special approval is required for compartmented data. [Refs. 20,32]

As mentioned earlier, physical requirements are based on the security operating mode, which in turn is determined by the sensitivity level. Hence, things like the physical facility security profile (FSP) should be based on the amounts and types of sensitive processing. [Ref. 13: pp. 12,40]

Security requirements apply to all systems handling classified information. Certain (usually older) administrative systems may not be subject to ADP security requirements. Stand alone administrative systems that do not process classified information do not have to be accredited. However, given teleprocessing requirements, ADP requirements, sensitivity considerations, and Privacy Act requirements, a LAN supporting administrative processing would probably have to be accredited [Ref. 13: pp. 9-12,18]. Moreover, cryptographic capabilities apply to any system with a confidential or higher classification. [Ref. 20: p. 36]

(2) *Designation.* Once sensitivity levels are set, detailed requirements for each system component can be identified. Also, all ADP operation and facility designations must be assigned. Nonsensitive systems are the only systems that don't require accreditation [Ref. 13: pp. 5-7]. Sensitivity level designations affect all aspects of the configuration, not only the physical aspects mentioned above, but also the control of system data [Ref. 32: pp. 3-8]. For example, there are different communications security requirements for different sensitivity levels that apply to the control of information transmissions [Ref. 20: p. 6]. Designation considerations include:

- **The type and sensitivity of information handled by each component.**
- **Who will access information at each network location.**
- **Physical location of network components.**
- **Who has offical control of specific data bases.**

(3) *Risk Management.* A formal risk management program must be established for each automated system handling sensitive defense information [Ref. 13: p. 5]. Risk management is intended to provide a means to identify, measure, control, and minimize weaknesses in the entire system configuration. The general objective is to prevent unauthorized system access and use. A specialized risk analysis should be conducted (by experts if possible) to determine vulnerabilities. The expenditure of resources to determine the most cost effective safeguards should be supported. [Ref. 13: p. 29]

c. Security Processing Modes

Security processing modes were discussed in Chapter III. They are the multilevel security mode, controlled security mode, system high security mode, dedicated security mode, and periods processing [Ref. 13: pp. 7-8]. Only system high and multilevel modes are presented (later) in this chapter to identify basic considerations. A detailed analysis of all the modes would prove to be lengthy. Additionally, both these modes are reviewed to provide background for an example presented at the end of Chapter V.

In contrast to standard Army guidance, DoD contractor security guidance only approves the dedicated, system high, controlled and concurrent security modes. The most notable difference is that the multilevel mode is not addressed. Nonetheless, concurrent processing of multiple classification categories closely resembles multilevel mode requirements addressed later in this chapter. Contractor security guidance applies to networks that are developed and/or operated by contractors. [Ref. 36: pp. 173-175,181-182]

Physical security requirements for contractor security modes must also be based on sensitivity. Above all, physical security protection must meet requirements for the highest sensitivity level processed by the system at each facility and remote terminal area. The only exception is that in an approved controlled security mode, remote terminals may be secured at the highest level for that site. Nevertheless all systems processing with a system high sensitivity of SECRET/CONFIDENTIAL must meet physical security requirements no lower than those required for CONFIDENTIAL. [Ref. 36: pp. 171-190]

d. Procedures

ADP system procedures that apply to LAN configurations involve implementation, access, facility construction, risk management, audits, and emergency plans.

(1) *Implementation.* First, minimum security standards for the network and then accounting and audit trails must be established in terms of implementation. Network security standards should then be used to develop system-wide security procedures. The procedures should be tested and analyzed along with system hardware and software to make sure they are compatible and are cost effective in terms of system performance. Once the system security hardware, software, and procedures are approved for operation, personnel should be trained. All user and operator training should include identification of security responsibilities as well as security procedure. [Refs. 2,13: p. 11]

Given a network manager and NSO are appointed in the design stages to assist and monitor design of security features, a TASO for each site should be appointed before implementation and testing at their specific site.

Mutual agreement on security responsibility between the organization controlling remote devices and the remote user organizations must be finalized before remote devices are implemented or allowed to access the system. Naturally, established security agreements and procedures are also required before internetworking [Ref. 13: p.5]. In addition, security/implementation requirements should be checked for each user organization and organization chain of command level. This allows identification of unique user requirements and priorities. For example, the type of organization (headquarters, post, etc.) affects user priorities in terms of who comes on line first and what they can do. Unique user requirements may also have an impact on implementation/installation schedules, testing, etc.

(2) *Access procedures.* Before access procedures are developed, vulnerable areas must be identified. Vulnerability information should be available from the system design or risk management documentation.

Controls for personnel access to ADP facilities and hardware during and after normal duty hours may include physical and/or manual procedures. Some examples are control of keys, control of combinations, continuous closed circuit TV monitoring, intrusion detection systems, exterior lighting during darkness, second access doors, and fencing. Access procedures should also include visitor controls that include escorts as a minimum, and depending on the processing mode, pre-arrival security checks. [Ref. 13: pp. 12-16]

LANs require protection of system documentation and media at the highest system classification level. In addition, file access is based on a "need-to-know". In addition, there must be sanitization procedures before and after contractors work at sensitive levels on any ADP system. [Refs. 13,36]

Password generation should also be based on sensitivity value of the system. Special care must be given to password generation, issue, and control. Transmission media channels for sending passwords should equal their classification level. [Ref. 13: p. 19]

(3) *Risk Management Procedures.* Above it is stated that a risk management program must be established for systems handling sensitive information. Risk management procedures are not standardized because every system is unique. Only phases of evaluation are standardized. This includes communications and emanations. As a result each command is responsible for it's own risk management activities. To determine the minimum level of protection needed, management must identify the resources to be protected and analyze the risk of espionage, sabotage, damage, and theft. [Ref. 13: p. 29]

(4) *Audit Procedures.* General ADP and network system accounting procedures are required for job accounting, resource accounting, and customer accounting categories. Audit and evaluation procedures required for the accounting categories can be separated into manual and automated rosters and logs, internal audits, and security verification programs. [Ref. 13: p. 25]

Data control is an important aspect of network environments and distributed systems. Networks require audit trail records for data as it is routed through the network. The network manager and NSO should always monitor who is on the system and what they are doing. In addition, each network user that processes information should have their own data control for their ADP equipment and location [Ref. 27: p. 2-1]. Minimum controls include:

- Watching schedules and workload arrival times.
- Automation summary reports to record receipt of data.
- Separate accounting procedures for classified products. This includes arrival records, summary reports, traffic classification logs, etc.
- Console logs. Identification of all users and time of access.
- Journalizing of each file accessed by each user and what the file was used for.

- Input control - determine the file accessed and and all restrictions (read, write, etc.).
- Identifiable output linked to the correct recipient.
- Printouts produced only at attended printers.
- Output control logs at remote devices.
- Scheduling procedures for user requests of large amounts of network resources.
- Logs must be retained for at least 60 days.
- Sensitive audit trail data must be retained for 90 days.
- Over-the-counter batch input/outputs must be reviewed before entering or leaving the network facility. [Refs. 13,27]

All system security incidents must be investigated [Ref. 13: p. 8]. Thus, the above audit procedures would be an important part of an investigation, as well as routine system control.

(5) *Emergency.* Emergency procedures for start-up, shut-down, and system failure must be planned because the network is especially vulnerable during unscheduled termination of operations. Operational security controls must be strictly enforced and intensified during these times. In other words, all areas must be secured at the highest operating mode level until normal operations begin. System software should provide minimal protection for minor interruptions like power surges, keeping them as transparent to the users as possible. When an emergency shut-down or system failure takes place an investigation must begin immediately to determine the cause, impact, and corrective measures (if any). Security plans/procedures are needed during system recovery to prevent further damage and vulnerability. [Ref. 13: pp. 24-25]

The Continuity of Operation Plan (COOP) requires off-site secure storage for sufficient copies of documentation material, data, and software to reestablish operations in the event the originals are damaged or destroyed. The sensitivity requirements for the storage area must be equivalent to the most sensitive item stored there. Proper off-site storage requires on-site and off-site rotation and storage of documentation, data, and software to ensure the most recent versions are available. System documentation should include network system recovery plans and procedures. [Ref. 13: pp. 24-25]

In addition, emergency text transmission procedures are required for national security information in the event secure modes are deactivated or not available. [Ref. 29: pp. 10-12]

2. ADP Hardware

a. Computers

In terms of the actual computer, security guidance is concerned with operation, management, and access of facilities and hardware.

(1) *Facilities.* It was mentioned above that the central facility must be secured to the highest system sensitivity level. In addition, direct access to the hardware within the facility must be controlled.

Note that supporting facilities (utilities, air conditioning equipment, etc.) should also be secured at the same level as the central computer facility. [Ref. 13: p. 15]

(2) *Access.* Physical access to ADP hardware is covered above in the system access section. Some additional requirements are listed below.

- Regular inspections.
- Restrict access to network control facilities.
- Tight control of identification devices (badges, keys, etc.).
- Change of keys and locks on a regular basis.
- Proper disposal of classified media and documents within a site.
- Applicable TEMPEST requirements to prevent unauthorized electronic access [Ref. 27: pp. 3-3 - 3-4]. TEMPEST is the unclassified name for the investigation and study of emanation compromise [Ref. 13: p. 78].

In terms of the "access" procedures in the system procedure section above, data file access is controlled by user passwords and identification procedures. Thus, access to the generic LAN is controled by passwords and procedures at the network center, while another set of controls may be required for access to specific computers or computer systems connected to the LAN. This would apply to situations where a user has access to a computer with a network interface, but the particular user does not have a need or clearance to access the network via that computer.

In addition, access to audit file information should be limited to the network manager, NSOs, and network center operators with a need-to-know.

In certain situations a system may connect to system(s) with a lower security operating mode. The system with the lower security operating mode must use approved disconnection techniques whenever sensitive processing exceeds the classification of the "connected" system. The same basic requirements needed at the system level apply to the component level (sanitization, etc.). Contractors can only use software disconnects for sensitivity levels at or below SECRET. The network manager and NSO should predetermine specific channels and/or transmission links for both hardware and software disconnects so they can be monitored during the disconnect. [Refs. 22,36]

In terms of sensitive information, "privately owned computers will be used only in a stand-alone configuration." Privately owned computers cannot be used in a LAN, network, or any type of remote connection to a mainframe configuration unless it is first accredited. Understandably, all information processed becomes property of the Army. The objective is to prevent penetration of a secure area or ADP facility. Any PC could contain emanation collection equipment, or if connected to a system, enable unauthorized collection, destruction, or alteration of information. In contrast, PCs owned or leased by the Army can be connected to any network or Army stand-alone system provided they meet system accreditation requirements, assuming Army owned PCs are secured and controlled properly. [Ref. 13: p. 10]

b. Terminal Devices

Understandably, the sensitivity of information processed determines terminal device requirements as well as other component requirements. General ADP terminal requirements that apply to the generic configuration are physical area, access, emergency, and accreditation requirements.

(1) *The Physical Terminal Area.* Networks terminal equipment must be protected before and after duty hours [Ref. 13: p. 14]. Normally,

> remote terminal area requirements will be based upon the highest classified and most restrictive category and type of material which will be accessed through the terminal under system constraints. [Ref. 22: p. 16]

However, remote terminals in systems controlled or under development by contractors, must continuously operate in the highest security class except for terminals approved for the controlled security mode. Basic physical needs are similar to the ADP hardware and general system considerations addressed above (lights, locks, construction, etc.). [Ref. 36: pp. 177-178]

Terminal media storage is especially important in LAN configurations where the remote terminal device is far from the network center. In remote terminal areas all disk packs, tapes, etc., as well as terminal devices, must be secured under the maximum approved security level for the remote location. [Refs. 13,22]

(2) *Terminal Access.* Direct access to a terminal device at any location can be controlled by a combination of time-outs, locking mechanisms and identification verification. Logon time-outs must be based on sensitivity levels. Physical and software terminal locking and unlocking must be controlled by system operators and authorized by the ADP system security officer (ADPSSO), terminal area security officer (TASO), or a network security officer (NSO) [Ref. 13: pp. 18,21]. Thus, access identification is accomplished before processing begins. [Ref. 22: p. 16]

Disconnect situations were covered under computer access above. Microcomputers and smart terminals approved for temporary connection or disconnection procedures, must undergo some type of memory sanitization before and after connection. By consequence, accoustic coupling should be minimized or eliminated because it is harder to audit and control. [Refs. 13,36]

Internetworking requirements mentioned above for computer hardware also apply to terminals. Terminals accessing a system or network must meet that networks minimum requirements and be approved by network authorities.

Lastly, terminals that access commercial time sharing computers or networks, must have a lockout mechanism or be located in a separate secure room. Accredited terminals used for access of commercial systems should be sanitized before accessing a classified network. Terminal software and hardware interfaces into the same network must also meet accreditation approval. [Ref. 13: p. 14]

(3) *Emergency.* The same general requirements mentioned above apply to terminals in terms of start-up, shut-down, and failure procedures. Remember, this includes full documentation and investigation of system failures and emergency shut-downs. [Ref. 13: p. 24]

(4) *Accreditation.* One major point concerning terminal device accreditation is in terms of its relationship to the system or network configuration. In short, Chapter III of the thesis mentioned that terminals, PCs, micros, minis etc. connected to a system more than 50 percent of the time must be accredited with the system [Ref. 13: p. 9]. Thus, terminals that access a network must have accreditation equal to the networks requirement for the sensitivity processing level, if they are not accredited with the system. Accreditation is covered in Chapter V of the thesis.

3. Transmission Hardware

a. General Transmission Media Considerations

Transmission media considerations that apply to LANs are ecryption, non-encryption security methods, telecommunications plans, teleprocessing audit controls, and communications security monitoring.

(1) *Encryption.* Encryption is transforming information into a code to conceal its meaning. End-to-end encryption is encryption of information at the origin, before it enters the transmission medium, and then decrypting at the destination after it leaves the transmission medium. Link encryption is "the application of on-line crypto-operations to a link of a communications system so that all information passing over the link is encrypted." [Ref. 13: p. 74] Encryption applies to confidential as well as other higher classifications, and is used to prevent unauthorized access of transmission media or electronic emanations. [Ref. 20: pp. 36-37]

All telecommunications transmissions of ADP "record" data must be secured by approved encryption in cryptosystems or by PDSs [Ref. 29: p. 3]. Moreover, all telecommunications must meet communication security criteria equal to the information security requirements, when supporting ADP systems. [Ref. 32: pp. 6-7]

Systems under contractor control and/or development that process classified information must be encrypted for both inter-facility and intra-facility transmission links. However, an approved level of physical security can be substituted.

Other measures that can be used in addition to encryption include a PDS, authentication, proper operator skills and discipline, and general communications security awareness. PDSs are discussed under non-encryption methods. Authentication is the process of verifying the eligibility of a system (or network) user to access information. [Ref. 13: p. 72].

(2) *Non-encryption Methods.* In a multichannel telecommunications system (and our generic LAN), the interconnecting transmission links that carry classified data and pass through unrestricted areas must be protected. Thus, a LAN configuration may meet PDS approval requirements for classified processing if it is within a controlled area with appropriate physical safeguards. If not, physical protection is required for all lines routed outside the facility . PDS physical protection requirements include:

- Special routing, physically isolated from other non-PDS cable media.

- Cable media must be routed within a secure perimeter or have guard patrols assigned.
- Cable media must be contained on the installation under the using commander's control. [Refs. 13,29]

Because of varied security techniques, locations and applications, each PDS will have unique requirements requiring evaluation on a case-by-case basis by approval authorities. [Ref. 29: p. 10]

Disconnect procedures mentioned earlier for protecting classified material by hardware and/or software methods, may be authorized by the designated approving authority. [Ref. 32: p. 7]

(3) *Telecommunications Plans.* Telecommunication plans referenced contain general topics, not specific security information. Still, ADP communication support plan requirements, that are a part of the telecommunication plan, may enhance LAN security planning. Security plans can have an impact on performance and cost effectiveness.

For instance, encryption requirements may have an impact on the communication support plan. Encryption requires one more interface process for a transmission link, resulting in a slow down in network responsiveness on the encrypted links. Also, a given encryption process may require that security-oriented headers be added to transmission packets resulting in a net decrease in efficiency. In addition, there is extra cost associated with extra components. In sum, the communication support plan includes data transmission formats, area and range of transmissions, volume of data, and transmission rates with the associated security requirements. [Refs. 23,35]

In terms of internetwork planning, all requirements for the generic configuration's gateways (and other interface components) would have to meet the security requirements of the network to which it was going to be connected.

(4) *Teleprocessing Audit Controls.* Batch teleprocessing systems must be auditable and controllable. Accounting procedures include internal audits and transaction logs. These procedures would be applicable to a LAN configuration supporting batch oriented functions. Remaining teleprocessing audit controls are covered above under system audit procedures. [Ref. 13: p. 25]

(5) *COMSEC Monitoring.* Communications security (COMSEC) monitoring is not required but it may provide information for improving network and telecommunications security. National Security Agency (NSA) approval is needed. [Ref. 30: pp. 4-5]

b. Interface Hardware

There are no specific LAN device requirements mentioned for interface components. Interface requirements would parallel standard ADP or telecommunications requirements depending on the device characteristics. For example, a controller could resemble a minicomputer and would be subject to the same secure protection. Naturally, network and telecommunication interoperability and standardization should be a goal of all services and agencies. Inter-agency awareness is required to accomplish this, so requirements of all agencies must be reviewed whenever any internet is planned. [Ref. 13: p. 32]

Even though each organization involved in a telecommunication network must be aware of each other's security requirement, there is one organization that provides approval. From all information presented, the system supporting the most sensitive processing has the ultimate security authority. [Ref. 22: p. 20]

4. Software

The software requirements addressed by the guidance reviewed for this thesis is ADP oriented; there was no mention of network protocols. The purpose of this thesis involves identifing security guidance pertaining to LANs. Thus, general statements about utility, application, and operating system software are presented here with comments about their relation to protocols.

a. General System Software.

Utilities, executive routines, security routines, and operating systems all support the objective of obtaining a secure system. In general, each must maintain separate user and master modes, identify and verify terminals before they are allowed to process, provide time outs, maintain audit trails, etc. The ultimate goal is prevention of unauthorized access. Thus, this type of software must be protected and controlled at the highest sensitivity level associated with the system, whether it is located on or off (disk, tape, or other media) the system. Protection levels remain in effect as long as the software is used on the classified system. These restrictions also apply to contractors.

Use of software security packages should be based on cost versus level of security protection provided. Moreover, classified data cannot be protected by commercial software alone.

b. General Operating System Functions

In simple terms a computer system is controled by the operating system which in essence, is a collection of system programs. The operating system and associated system software provides many of the basic internal security features required for a computer and the system in general [Ref. 13: p. 75]. Basic requirements include partioning areas of memory by classification level with capabilities for control of interrupts in a way that will enable preservation of data integrity within memory. Also, an operating system should have the capability to provide memory bounds checking when information is transferred. Identification of all users and devices active in the system must be provided.

c. Application Software

Commercial/purchased software approved for unclassified or lower, or contractor produced software, can only be introduced into the system during classified processing in a read-only or write-protected manner. [Ref. 36: pp. 182-183]

Data base management systems (DBMS) must include protection at least down to the record level to be used for classified data, but the element or field level is preferred. Also, a DBMS must have a journalizing capability and produce it's own audit trail if it by-passes the system audit trails. The goal is to be able to track activity to the lowest possible level [Ref. 13: p. 10]. It should be noted that software audit procedures (logs, files, etc.) can be automated, manual, or a combination of both [Ref. 22: pp. 26-29].

d. Protocol Software

For the purpose of this thesis, interface software refers to protocols, but before proceeding with protocols a review of some definitions are in order. Executive software controls include input/output controllers, operating systems, and ADP equipment. Utility software handles routine merges, sorts, and other processes for executive and applications software. Application software is strictly functional user applications. Operating systems consist of a set of utility and executive routines that control hardware resource allocation and programs, i.e., the basic functions of the computer system. [Refs. 3,13: pp. 303,71-78]

In Chapter II, a protocol is defined as a set of rules that govern data communications transmissions. Actually, the rules transform into requirements and specifications for the executive, utility, and application software that control network interaction. First, individual systems accessing the network must have their own operating system that handles protocol hardware and software requirements. Included would be ADP and transmission interface requirements. In turn, ADP and transmission interfaces would be required to have appropriate security features. This provides functionally secure transmissions throughout the system. Hence, the protocol causes a network synergy. In other words, when all specifications are met, the protocol rules produce an "operating system effect" that controls the entire network. Thus, the protocol is protected via the implementation of the other system components and their corresponding security requirements.

C. PART 3: MULTILEVEL OPERATION MODE - GUIDANCE REQUIREMENTS FOR NETWORK COMPONENTS

Component areas addressed in this section are multilevel security mode specific. Reference the previous sections about general requirements for topics not covered here.

1. Configuration Considerations

The multilevel security mode consists of concurrent access to various types and categories of classified information, concurrently stored and accessed by users with different clearance levels and need-to-know. Consequently, many users may not possess a security clearance that equals the level required for the most sensitive information processed and stored on the system.

The operating system and associated system software is the component that handles multilevel processing [Ref. 13: p. 75]. However, there are multilevel LAN configurations that use a combination of hardware and software to obtain a secure multilevel environment [Ref. 37: p. 75]. It is possible that either of these hardware/software configurations could be accredited.

In addition, network configurations are considered more vulnerable than other ADP configurations because they "require precise control of complex interactions, and the probability of system error is greater." [Ref. 13: p. 7] In other words, the distributed processing and storage of data makes the system more vulnerable. Password generation, for instance, may be more complicated to manage on a network than a stand-alone ADP system. Yet, in a multilevel network configuration even more attention to password generation, assignment, access restrictions, etc. is required. [Ref. 13: p. 19]

2. Sensitivity and Operating Mode

Multilevel security processing is prohibited for any CS1 or CS2 system without the written approval of the Assistant Chief of Staff for Intelligence (ACSI).

This mode would be appropriate for separating SECRET/CONFIDENTIAL (CS3), highly sensitive (includes Privacy Act data), sensitive, and nonsensitive information.

As mentioned earlier, contractor security guidance does not literally mention multilevel security, although, it does mention concurrent processing of multiple classification categories. Concurrent processing means proper and controlled segregation of security classifications. It refers to storage of more than one security classification within the same system. As a result, it does not specifically address actual user interaction. The security requirements parallel multilevel guidance. [Refs. 32,36]

3. Procedures

In a multilevel environment continual system reviews are required to ensure that system access control limits users to only the resources they require to perform their duties and to information they "need-to-know". In terms of passwords, classification is "according to the system access to which the user is authorized and the terminal from which the activitiy is initiated." [Ref. 13: p. 19] Moreover, remote terminals can have access to the system "only from terminals designated and protected for the appropriate level of classified processing." [Ref. 13: p. 19]

4. Software - Operating System

Different multilevel operating systems have been approved at different sensitivity levels by NSA. Yet, a particular multilevel operating system may not be approved for all applications at a given classification level. Moreover, the "system effect" may reduce over all multilevel sensitivity performance. As a result, a multilevel operating system approved for a particular sensitivity level may not maintain that sensitivity level for all applications.

D. PART 4: SYSTEM HIGH MODE - GUIDANCE REQUIREMENTS FOR NETWORK COMPONENTS

Component areas addressed in this section are system high security mode specific. Reference previous sections of this chapter, excluding the multilevel section, about general requirements for topics not covered here.

1. Configuration Considerations

A system high configuration requires all system components to be protected at the highest security processing level. All personnel accessing the system have the "system high" security clearance, but may not have a need-to-know for all information on the system. [Ref. 13: p. 75]

The system high mode lends itself to the "peripherals/systems" approach which can be applied to the generic LAN configuration. The peripherals/systems approach requires that all security considerations must be addressed during development, implementation, and operation in terms of all components. Remember that temporary waviers are possible. [Ref. 13: p. 32]

2. Sensitivity and Mode of Operation

Guidance requires that need-to-know controls must be contained within the ADP system's operating system hardware/software. Unlike true multilevel operating system requirements, system high does not require memory partitioning or other memory unique control functions in the multilevel sense.

A LAN configuration operating in a system high mode connected to a system or network with a higher classification, could be physically disconnected at the gateway/interface during processing at the higher classifications. Likewise, a system or network connected to a LAN with a higher classification could be disconnected when the processing classification level of the LAN exceeds it's own. [Refs. 13,36]

Another possible mode of operation identified by guidance involves actually temporarily adjusting the total system operation to a higher security level if all security requirements for that level are met and approved. The system must then be returned to it's original state (declassified) when processing is complete. [Ref. 32: p. 4c]

System high operating mode restrictions include:

- No SIOP-ESI processing.
- SCI can be processed when requirements of DIAM 50-4 or DOD C-5030-58M are met.
- Adequate security for CS2 and CS3 systems.
- Can be specifically approved by the accreditation authority for "highly sensitive" systems. Password security is mandatory.
- Can be specifically approved by the accreditation authority for "sensitive" systems. Password security is mandatory. [Ref. 13: pp. 7-8]

Thus, procedures for password generators and control should be carefully planned and implemented.

E. SUMMARY

LAN guidance requirements covered in ths chapter must be applied to a particular configuration so the proper security features can be mapped into the hardware, software, transmission medium and interfaces, and the overall system, during design and implementation. In doing this, the ultimate degree of access flexibility and system security will depend on the sensitivity level and mode of operation. The objective is to apply security guidance requirements to a particular LAN to obtain accreditation.

V. LOCAL AREA COMPUTER NETWORK APPROVAL METHODOLOGY

A. INTRODUCTION

Once the network objectives are set and risk management analysis is complete, an adequate sensitivity level can be determined that eventually leads to a security operating mode for the network. The final operating mode designation is approved only after it meets the guidance requirements presented in Chapters III and IV. Chapter V refocuses the guidance reviewed in the previous chapters by highlighting some important areas of the guidance and the generic configuration in terms of the accreditation process. The purpose is to point out general network areas that must be addressed for accreditation and their basic impact on the configuration/system.

First the accreditation process is defined and summarized in a general sequence of steps. This includes a review of accreditation policy makers; organizations; and network and ADP security positions at the operational level. The last part of the accreditation review addresses the part of the accreditation process covered by the thesis.

System configuration considerations and requirements for sensitivity, network control, management, procedures, significant applications, and future upgrades are covered next. More system component considerations are then presented for hardware, software, and terminals.

The chapter ends with two examples of alternatives that illustrate how the designated network security mode can affect the configuration design.

B. ACCREDITATION OVERVIEW

1. Background

a. Definition

In a pure sense, accreditation is the actual "approval" to process sensitive or classified data. In the real world of automated system development and implemention, accreditation is the process of collecting and analyzing security related information for approval of security requirements for networks, ATSs, and computer systems. It includes submission of specific information to an approval authority for review and analysis, and any required system review meetings and inspections. The process ends when the accreditation authority grants a specific system permission to process specific level(s) of sensitive information. The accreditation authority is the official designated to approve an automated system for processing of sensitive information. As mentioned in Chapter I, The accreditation authority for systems processing critically sensitive levels of information is the HQDA or MACOM commanders (general officers), depending on the system. For highly sensitive information, installation, post, or field operation commanders can be the accreditation authority. At the sensitive level the heads of the data processing activities (DPA) or centralized office automation agencies may be the accreditation authority. Nonsensitivity systems do not need accreditation. [Ref. 13: pp. 6,30,71]

b. General Accreditation Goal

The goal of accreditation is to ensure that the system has security features that correspond to the level of protection required for information processed by the system. The idea is to provide enough flexibility in accreditation requirements so that the protection is affordable and has minimal impact on system efficiency and capacity given the unique circumstances of the system.

c. Applicability

Accreditation is applicable to all Army networks as well as computer DPAs and ATSs, except for:

- Computers embedded in combat weapons systems.
- Unclassified data or signals processed on analog computers
- Programmable calculators and mathematical processors without external storage and text processing capabilites. [Ref. 13: p. 30]

d. Categories

Sensitivity levels identified in Chapter III are used to categorize automated systems. The variation in types of systems, functions, and installations requires different accreditation standards and procedures for each sensitivity level as well as each unique system. Single-sensitivity level system accreditation is relatively straight forward in terms of security requirements - maximum category requirements apply to the entire system. However, for multiple sensitivity levels the system will be accredited at the highest level, but subsystems may establish policies and procedures to operate at their individual sensitivity levels. [Ref. 13: p. 30]

2. The Accreditation Process

Accreditation is explained in AR 380-380 and applies to all Army DPAs, ATSs, and networks as stated above. All accreditation information covered in this chapter is found in AR 380-380. The basic requirements of the accreditation process are summarized in the next section.

C. ACCREDITATION REQUIREMENT SUMMARY

The basic requirements of the accreditation process follow. A general flow diagram of the process that represents these requirements is illustrated in Figure 5.1. [Ref. 13]

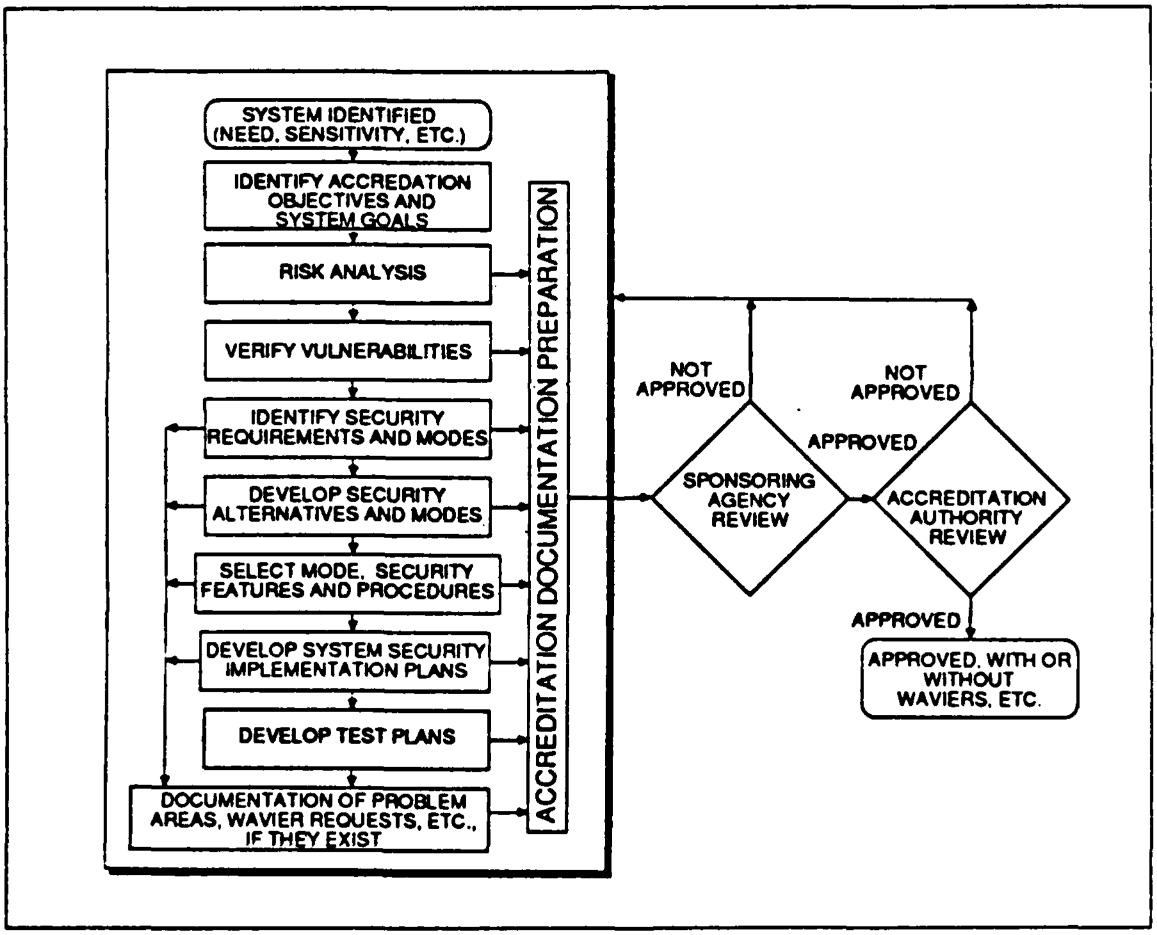

SYSTEM IDENTIFIED (NEED, SENSITIVITY, ETC.)
IDENTIFY ACCREDATION OBJECTIVES AND SYSTEM GOALS
RISK ANALYSIS
VERIFY VULNERABILITIES
IDENTIFY SECURITY REQUIREMENTS AND MODES
DEVELOP SECURITY ALTERNATIVES AND MODES
SELECT MODE, SECURITY FEATURES AND PROCEDURES
DEVELOP SYSTEM SECURITY IMPLEMENTATION PLANS
DEVELOP TEST PLANS
DOCUMENTATION OF PROBLEM AREAS, WAVIER REQUESTS, ETC., IF THEY EXIST
ACCREDITATION DOCUMENTATION PREPARATION
NOT APPROVED
NOT APPROVED
APPROVED
SPONSORING AGENCY REVIEW
ACCREDITATION AUTHORITY REVIEW
APPROVED
APPROVED, WITH OR WITHOUT WAVIERS, ETC.

Figure 5.1 General Accreditation Process and Requirements.

1. **Validated System Need and Requirements**

Identify and validate the need for the network and determine system requirements. In short, a need for a system has been determined because of a deficiency, outdated system, technical opportunity, change in threat, or a chance to reduce operating costs. Moreover, a tentative system is at least designed.

2. **Statement of Accreditation Objectives and System Goals**

Preparation of a statement of accreditation objectives and system goals is required. It must include a validation and review of the need for the system, the nature of mission, and other factors concerning accreditation.

3. **Risk Management Analysis**

Conduct a risk management analysis to identify risks and countermeasures, and then formulate a detailed cost and benefit analysis. When complete, a review is conducted so commanders/managers can determine system sensitivity and appropriate countermeasures. Risk assessment and analysis must be documented and protected at the appropriate sensitivity level.

4. **System Configuration and Operation**

Documentation must be compiled with the key security considerations forming the basis of accreditation, and a detailed description of proposed operations. Note that planned procedures used between processing modes/levels must be included for Periods Processing and Controlled Security Modes.

5. **Implementation Plans**

In addition to the initial implementation plan, and review plans, similar plans for additional security features must be developed and include near term goals, long term goals, overall mission related goals, and future plans in relation to the organizations the system supports.

6. **Standard Test and Evaluation (ST&E)**

ST&E plans must include purpose, scope, objectives of the test, and test methodology. Test team organization and responsibility assignments must be identified. Actual testing must validate all procedures and data processing (includes applying inaccurate data), and challenge security features with and without knowledge of site personnel. Emergency testing procedures must include unscheduled shutdowns as well as other adverse conditions.

7. **Plans for ST&E Results**

Separate plans for results of ST&E must also be documented. Test findings must include comparison of expected results to actual results. Test findings, conclusions, and recommendations must be submitted with accreditation documentation.

8. **Problem Areas**

A statement of continuing problem areas must be prepared for vulnerabilities not fully covered (or not addressed) by security features. Waviers or accreditation disapproval may result.

9. **Other Documentation**

Documentation description of the DPA, ATS, or LAN such as reports of outside agencies, FSP, ST&E, etc. is required.

10. **Accreditation Documentation**

Preparation of accreditation document in the format presented in Appendix I of AR 380-380 is mandatory. It must be prepared and submitted to the accreditation authority so she/he has enough time to review it before the formal review at the accredidation level. The accreditation document will contain information identified in the requirements above and also factors motivating accreditation and nature of the mission, reasons for rejecting other system and security alternatives, and attachments. Required attachments include the automated data processing system security officer (ADPSSO) appointment orders, copies of all inspection reports, and supporting documents referenced by the accreditation document.

11. **System Operating Level Command Review**

Formal command authority review at the operating level is required. A MACOM statement must be attached stating the accreditation document package was reviewed and examined, but only when the accreditation authority is the ACSI, HQDA, or higher. A recommendation must be included at these levels.

12. **Accreditation Authority Review**

Formal command authority review by the accreditation authority resulting in a decision is mandatory. If approved, a written accreditation statement is required from the accreditation authority. Or, the system could be disapproved with a temporary wavier or exception. A future accreditation review is required to ensure discrepancies are corrected. Most of the process must be repeated if the wavier is disapproved.

13. System Implementation and Operation

Implement system or begin operations (existing system). At this point, the operating site must maintain a copy of the formal accreditation document. Note that the accreditation process must be complete before sensitive or higher level operations can begin and the appropriate authority must issue a formal dated statement. In addition, the NSO must periodically review, test, and reevaluate network security for periodic accreditation reviews.

D. ORGANIZATIONS INVOLVED WITH APPROVAL AUTHORITY

Accreditation is addressed at many levels of the Army, from the commanders, managers, and staff who develop and implement policy to the commanders and operators of ADP systems.

The accreditation authority for a specific system is selected from the chain of command that the system falls under. The level of rank (and organization) in the chain is determined by the sensitivity designation of the information in the ADP system or network. The sensitivity levels and corresponding accreditation authority selection are addressed below. For example, in systems processing critically sensitive levels of information, the accreditation authority would be a general officer from the HQDA or MACOM. The system sensitivity and corresponding accreditation authority levels are summarized below. [Ref. 13: p. 6]

- CRITICALLY SENSITIVE
  - CS1 -- Headquarters, Department of the Army (HQDA)
  - CS2 -- MACOM commanders and heads of DA staff elements
  - CS3 -- Same as CS2 except can be delegated to general officer commanders of their subordinate elements.
- HIGHLY SENSITIVE -- Commanders of installation, post, field operation support activities, or staff support activities.
- SENSITIVE -- ADP and centralized office automation activity heads.
- NONSENSITIVE -- Accreditation not required.

NOTE -- Multilevel systems require ACSI approval regardless of sensitivity level (above NONSENSITIVE).

E. SUMMARY OF ADP SECURITY POSITIONS

General lists of the ADP policy and security hierarchy, and ADP operating level security positions are listed in this section for the reader's information.

a. ADP POLICY AND SECURITY HIERARCHY

- ASSISTANT SECRETARY OF THE ARMY (FINANCIAL MANAGEMENT) (ASA (FM)) - senior policy offical for Army ADP.

- ASSISTANT CHIEF OF STAFF FOR INFORMATION MANAGEMENT (ACSIM) - manages overall Army automation program.

- ASSISTANT CHIEF OF STAFF FOR INTELLIGENCE (ACSI) - develops and implements the AASP; ensures compliance with ADP directives; identifies and addresses ADP problems; determines applications of new technology; provides guidance for preparation of new systems; and manages overall automation security.

- HEADS OF MAJOR COMMANDS (MACOM) - manage/administer all aspects of ADP within their relm for key ADP personnel which include data processing activity (DPA) commanders and managers, SSMs, ADPSSOs, NSOs, and TASOs.

- SECURITY PROGRAM MANAGER (SPM) - appointed for each HQDA agency and MACOM; manages AASP; appoints SSMs and ATSSMs.

- DEPUTY CHEIF OF STAFF FOR PERSONNEL (DCSPER) - provides policy and procedures for physical security plans; advises ACSI on ADP related security fraud.

- COMMANDING GENERAL, U.S. ARMY INTELLIGENCE AND SECURITY COMMAND (CG, INSCOM) - implements Automated Data Processing System Security Enhancement Program (ADPSSEP); provides tech guidance and assistance for communications security, emanations control, and counter intelligence.

b. ADP OPERATING LEVEL SECURITY HIERARCHY

- SYSTEM SECURITY MANAGER (SSM) and Automated Telecommunication System Security Manager (ATSSM) - advisor to commander on ADP security matters; integrates security actions of individual system ADPSSOs and TASOs; maintains inventory of post, installation, and tenant ADP accreditation, including their status.

- SYSTEM SECURITY CONTROL OFFICER (SSCO) - appointed by organization as primary point of contact for all security matters for central system development activities; reports to ATSSM; responsible for all aspects of policy and procedural guidance for systems assigned to him/her.

- AUTOMATIC DATA PROCESSING SYSTEM SECURITY OFFICER (ADPSSO) - basically the same responsibilities as a SSCO, except for ADP equipment at a single site; would report to or coordinate with a SSCO if the site was connected to a network.

- NETWORK MANAGER - designated when two or more ADP systems are linked together for network or distributed operations.

- NETWORK SECURITY OFFICER (NSO) - responsible for all aspects of network security; reports to the network manager.

- TERMINAL AREA SECURITY OFFICER (TASO) - responsible for all aspects of terminal and network security in an assigned area; may report to SSM, ATSSM, SSCO, ADPSSO, or NSO depending on the type of system the terminals are connected to.

F. THE ACCREDITATION PROCESS - SYSTEM CONFIGURATION AND OPERATION

This thesis has addressed the security guidance considerations that apply to the system configuration and operation; the fourth requirement in the overall summary of requirements described above. In short, the thesis is intended to serve as guide for identifying network guidance requirements for the system components addressed in the fourth item of the requirement summary above. In a real network the requirements would be applied to the specific components and their specifications. Here, given the generic configuration described in Chapter II, actual application considerations will be general.

Activity for satisfying the fourth requirement item in the summary above begins with a description of proposed operations. This includes explaining actions taken to minimize risk and procedures to be used throughout the network. Moreover, areas addressed must include description of system hardware and software, significant applications and system interfaces, location of all remote devices, and features of operational and security modes in existence and to be implemented including requests for waviers. Features that must be included in accreditation documentation are listed below. [Ref. 13: pp. 40,58]

- Security features and management of components.
- Major executive and application software.
- Encrypted/non-encrypted terminals and devices.
- Procedures for log-ons, changing sensitivity processing levels (periods processing), etc.
- Communications - transmission links and associated components.
- Personnel - not addressed by thesis.
- Security of system documents/documentation.
- Physical and Environmental security.
- A completed Facility Security Profile (FSP).

Also, problems must be identified that are disruptive of accreditation processes, tasks, and time tables. In terms of the system, acceptance of each risk that cannot be minimized must be identified with a description of the situation and waiver request (if appropriate). [Ref. 13: p. 58]

Once descriptions are complete, an initial implementation plan must be completed. Such a plan is beyond the scope of this thesis, however, it must provide a description of:

- Security phases.

- **Milestones.**
- **Initial/final operational capabilities.**
- **Task interdependencies.**
- **Organizations responsible for accomplishing milestone-related tasks [Ref. 13: p. 58].**

In addition to normal accreditation reviews, reaccreditation is required for all networks and ADP systems within 3 months when any of the following occur:

1) Major system or "mainframe" addition or replacement.
2) "An increase in sensitivity category or level."
3) "A significant change in the DPA/ATS which requires a more complex mode of operation (para 1-13), or a more complex operational service mode (para 1-11)."
4) Major operating system or executive software.
5) Internal and external security violations, integrity violations, or any situation that invalidates the accreditation.
6) Significant changes to the DPA/ATS physical structure. [Ref. 13: p. 31]

G. METHODOLOGY IN RELATION TO SECURITY REQUIREMENTS: SYSTEM CONFIGURATION CONSIDERATIONS/REQUIREMENTS

In sum, guidance presented in the earlier chapters is in general terms so it can be easily applied to most automated systems and at the same time provide the appropriate flexibility. Thus, the guidance should apply to most aspects of each system component. However, because networks are not specifically addressed, LANs must derive guidance from standard computer (ADP) and teleprocessing requirements. This indicates that much of the specific responsibilities for security requirement determinations, for accreditation of a specific network, are left with the ultimate system user/sponsor.

The thesis has presented the "generic" LAN configuration and associated components (Chapter II) to match the "generalness" of the guidance reviewed. This approach generates more system level considerations because specific vendor hardware/software analysis is beyond the scope of this thesis. Consequently, system considerations and requirements for sensitivity, network control, management, procedures, significant applications, and future upgrades are covered next.

1. Sensitivity

It is mentioned throughout this thesis that sensitivity is the driving force behind any secure processing mode. As a result, the official sensitivity designation sets the scope for system development and implemention in terms of accreditation.

In the generic LAN, as in any system, the information contained therein, is the ultimate vulnerable area. All guidance pertaining to sensitivity designation determination applies. The basic security sensitivity level definitions (critically sensitive, highly sensitive, etc.) and security processing mode (multilevel, system high, etc.) requirements are clear. In a network context, LAN sensitivity mode determination would involve the same considerations. Thus, there are no gaps in the "non-network" oriented guidance in terms of functional sensitivity determination.

The areas addressed in the first three requirements in the accreditation requirement summary should result in an adequate system sensitivity designation. Nonetheless, the component parts of the network should NOT be ignored. In other words, sensitivity of each component part should be considered in terms of the overall system sensitivity designations. In doing this, it may be better to first concentrate on security needs for specific component areas to identify variability or constraints that would affect the overall system, before settling on a final system designation.

In terms of accreditation, the purpose of the system sensitivity designation is to protect information from unauthorized penetration via the functional sensitivity mode which is the most cost effective. Cost is used here in relation to actual system impact of the designation, not in terms of actual dollar cost. For example, the actual dollar cost would be the actual price of some cryptography hardware, while the impact cost might be the manpower, diverted from "productive" activities, required to manually distribute sensitive crypto-keys. Impact refers, for example, to how the sensitivity level might affect utility in terms of configuration design, operating procedures, and the range of system applications.

Each of the designated modes have different operating requirements which in turn vary the cost of a desired configuration. More sensitivity levels and access flexibility would require a more complicated system given todays guidance and technology. The dedicated mode would affect the generic configuration the least because there is one sensitivity level dedicated to one group of users. System high is similar to the dedicated mode with the exception of extra procedural controls required to determine the "need-to-know". In contrast, the controlled security mode would require, for example, more procedural controls and more complicated audits, i.e. "cost" more. Moving on to the other end of the spectrum, multilevel would cost more in terms of the number of sensitivity levels and the way that the multilevel environment was achieved. In other words, via a true multilevel operating system; or separately configured LANS, for each level, acting as one system transparent to the user. In addition, extra approval activities are required. For example, the ACSI must know of intent to use a multilevel environment before milestone "zero". [Ref. 13: p. 7]

2. Network Control

Network control in the generic LAN context should be most concerned with device interfaces and connections. Administrative and electronic access, audits, and monitoring activities must be well planned and designed. The generic LAN requires a central control facility for tight control of these activities. In the generic configuration and other systems alternate control facilities may be desirable as well.

a. The Central Control Facility

Just as is a central computer room in a stand-alone ADP system, the network control center (NCC) is vulnerable in terms of physical and electronic access, and environment preservation.

All physical requirements for a normal ADP computer center apply to the generic LAN NCC facility regardless of which devices work together or separately in terms of network control and the classified operating mode. This includes proper construction materials and design of the building(s) and room(s), physical hardware protection, and TEMPEST shielding. Remember that the supporting utility facility must be protected at the same level as the NCC, i.e. system high. In addition, all requirements pertaining to facility access and physical storage of media, both offsite and in the facility, apply. A system high security environment must prevail in the NCC because it is the physical location that not only monitors and controls the network, but also maintains the network security features (audits, system software, etc.).

There is no gap in guidance in terms of physical central configuration control of a distributed system through a NCC because all the requirement areas mentioned above for standard ADP systems apply to the generic LAN. Thus, the NCC should be protected at the system high sensitivity level in the same way that a mainframe environment would be. Performance and reliability are enhanced when equipment supporting the control of the network are secure to a level that ensures continued operation at a given security mode.

b. Remote Control Facility

If the generic configuration did consist of an alternate control facility it would require the same basic requirements as the central NCC. It could serve as a back-up, alternate, or replacement when the central facility is destroyed or damaged.

Obviously, it would require the same type of network control components and therefore the same security requirements.

c. Interfaces

From a system standpoint, an interface could be a simple port on the back of a terminal, or some sort of trusted interface processor that performs buffering and security functions on the information passing to and from the system. Vulnerabilities are further magnified in terms of a gateway or bridge to another network. Vulnerable areas include penetration of interface software and possible signal emanations.

Requirements for encryption, disconnects, and a PDS apply to the generic LAN configuration in one way or another. Army communications security policy requires security by either PDS or encryption for automated sensitive information. In reality, a combination of varying degrees of both are acceptable depending on the system sensitivity level, the application, and the actual configuration. In some situations a disconnect is acceptable. As a result of this range and variablity, the accreditation process requires a description of significant interfaces.

Given the nature of the guidance reviewed, there are no direct references to ADP network interfaces, but from all information they are, again, treated in the same way as ADP and telecommunications networks. This point is a major concern because in a LAN environment a major interface, like a trusted interface unit or a gateway, has a major impact on the security of a LAN. These units control and restrict communication to and from various parts of the network. Thus, it is important that they are protected at the network system high. [Ref. 37]

Assuming the generic LAN will process sensitive data, as mentioned above, encryption, requirements for a PDS, or a combination of both will be required for accreditation.

(1) *Interfaces in a PDS.* Interfaces between all network devices and components require shielding and physical protection just as the other network components. In addition to the physical device or cable, the device ports can emanate signals that can be compromised. Thus, every port, interface device, transmission medium, as well as every ADP device must be physically shielded and protected.

Low voltage processors may be an alternative to tempest shielding in some applications. These processors do not need TEMPEST shielding because emanations are so weak, but any attached CRT screens would. Thus, low voltage processors may replace TEMPEST shielding in "black box" or stand-alone processing devices like controllers or interface units. In essence it would require system high protection with the only access being surveillance and maintence. [Ref. 35]

Note that the generic configuration (Figure 2.1) illustrates separate lines leaving the NCC. In reality, these lines would pass through a multiplexer and be routed by a single trunk line to other rooms and buildings (Figure 5.2). A trunk is a group of communications lines enclosed in a single casing that usually connects two switching centers or multiplexers. [Ref. 3: p. 381]

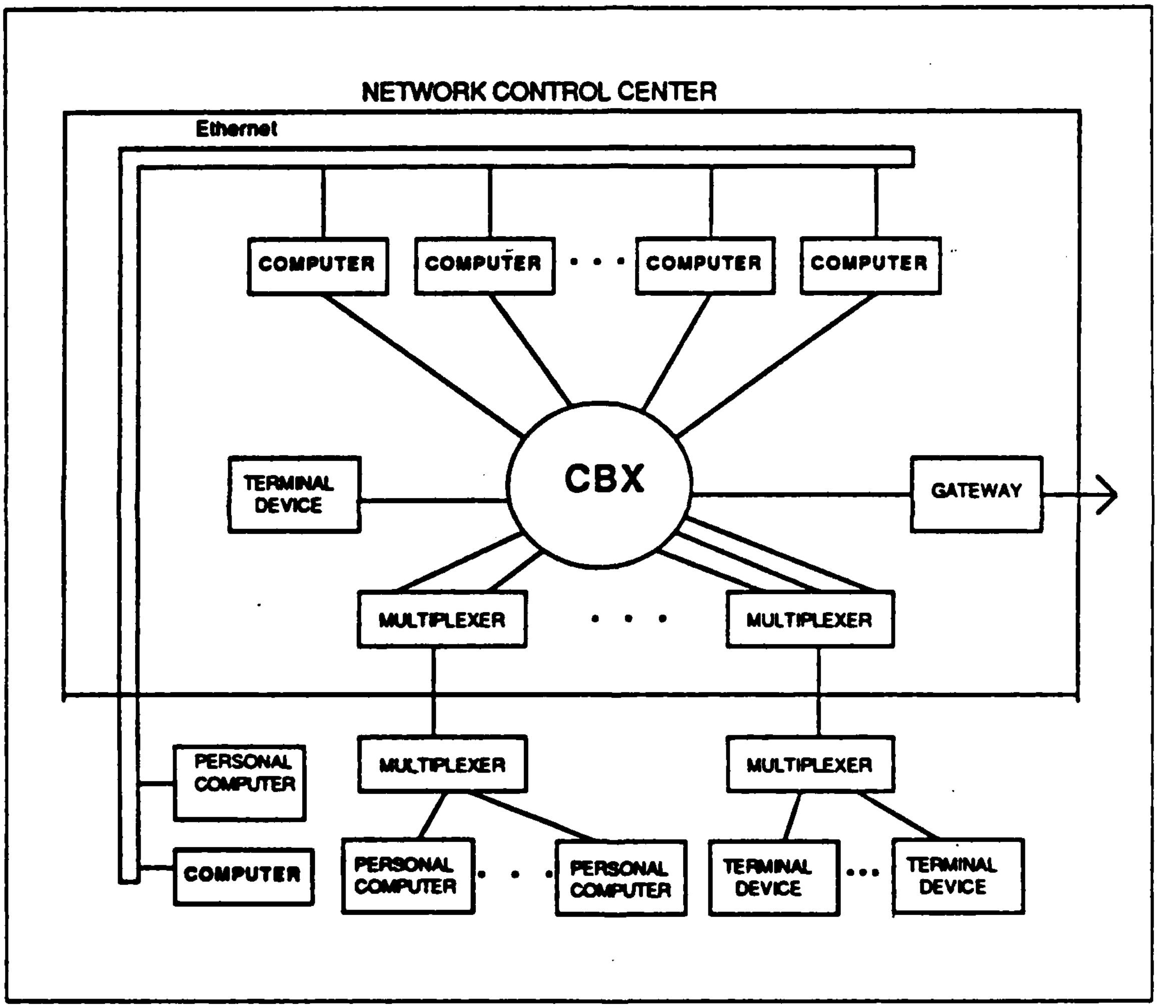


Figure 5.2 The Generic Configuration with Multiplexers.

(2) *Interfaces and Encryption.* Encryption is one of other major alternatives that has an impact on the system interfaces. Assuming the sensitivity level requires encryption for the entire system, an encryption device would be required for

each line going into or out of the CBX, as well as each device on the network (Figure 5.3). Extra fine tuning of the network would be required for synchronization between the encryption devices and the CBX, and all device interfaces on the system. Moreover, each encryption device requires a special key for encryption. An encryption key is a sequence of symbols that control the code scrambling mechanism within the encryption unit. The actual key could be a series or combination of symbols, letters, or numbers. A common procedure is to change the key at least on a daily basis. Without the correct key, a device cannot communicate because it would not be synchronized with the other devices. Synchronization is further complicated by the distance between devices. The farther any two devices are apart, the harder it is to synchronize. [Refs. 13,35]

(3) *Impact of System Interface Protection on the LAN.* In terms of the overall network configuration, interfaces are the glue that tie the system together. Thus their overall impact on network security must be addressed.

In a pure LAN PDS, physical protection of interfaces should not affect LAN performance in terms of through-put or efficiency. Extra procedures may be required to physically reach a device because it is physically protected or guarded. The major concern would be ensuring that metal protection devices do not emanate signals. For instance, power sources may require noise filters, and conduit may have to be composed of sections of nonconductive material. [Ref. 35]

In contrast to a PDS, a LAN that was entirely encrypted would experience an overall reduction in reliablity and performance in terms of slower data rates and response times. Historically, networks with cryptographic devices are less reliable than they would otherwise be, because cryptographic synchronization requires more maintenance and fine tuning. From a system view, cryptographic device is one more hardware/software fail point in the network. [Ref. 35]

An entirely encrypted network would also require procedures and plans for "crypto-key" changes and generation. As mentioned above this is critical, the key should be changed regularly because a site or device must have the right key to operate on the network. Crypto-key restart procedures would also be needed in case a key is lost by any network user. Still the most important procedures would be for the electronic or manual distribution of keys. Electronic distribution would require a specially secured and approved line. Above all, any "crypto" procedure, device, or software must be protected at the system high security level. [Ref. 35]

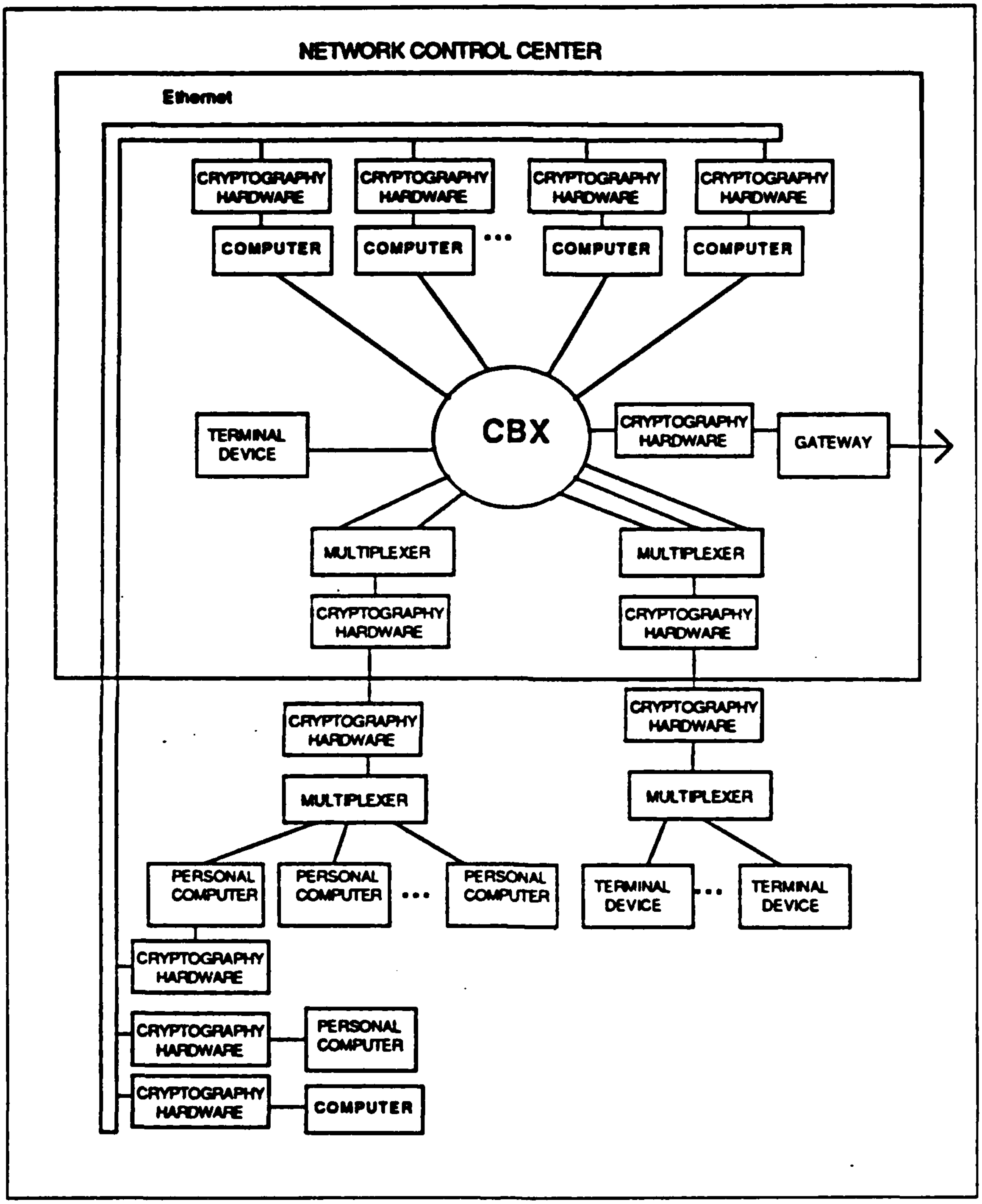


Figure 5.3 The Generic Configuration with Cryptography.

Do not forget that a partial or total combination of cryptography and PDS techniques can be used. The major advantage of cryptography is that encrypted information can be transmitted over any transmission link as long as the receiver has the same level of protection as the transmitter (and the right key). The major disadvantages of encryption were addressed above. Conversely, the major advantage of a pure PDS is that in most cases system reliability and efficency are not affected. However, every part of the network must be contained within a secured physical area and shielded. Thus physical access procedures and emanations may make access cumbersome.

d. Disconnects

Accreditation documentation must account for any disconnects planned in the system. Access and connection/disconnection procedures must be included for connecting to networks/systems of higher, lower, and equivalent security classifications. Moreover, the devices to be connected or disconnected and the type of disconnect(s) must be specified. Overall impact on operations should also be addressed.

e. Physical

Physical LAN considerations for accreditation are for the most part straight forward. It was mentioned in earlier chapters that descriptions and locations of all devices are required in the accreditation package. This includes floor plans as well as configuration diagrams like the generic configurations presented in this thesis.

If the generic LAN was to be secured by meeting only PDS requirements, TEMPEST shielding for all hardware and/or rooms and even buildings would be required. Again, depending on sensitivity, a combination of shielded rooms and unshielded rooms with shielded hardware, may exist within the same building. Cable media running outside of shielded rooms or buildings would also have to be shielded and protected. Moreover, special attention must be paid to certain types of conduit and other media protection devices because they can cause emanations. In addition, proper physical controls would have to be maintained in terms of area security. The physical area could range from a room to an area containing many buildings. [Ref. 35]

One major consideration is the physical placement of the NCC within a building, and depending on the physical distance from other network sites, on an installation. Obviously a central location within a sturdy building or within a protected area perimeter is ideal. Realistically LANs are not always located in an ideal environment. Variations in physical controls and access barriers may have to be adjusted to meet a given security operation mode. For instance, if a network was located in a building that was not located in a central position on the post, maybe emphasis on physical perimeter safeguards (fences, guards, lighting, etc.) along with the normal building security requirements, would meet accreditation needs. Remote sites would be subject to the same basic requirements as the NCC unless the network was operating in a controlled or multilevel mode. With more than one security mode, placement is still critical because any node or terminal is a penetration target, but less actual physical security would be required for sites approved to operate at less than system high. Remember placement and/or protection considerations for the network's power source are equivalent to the NCC.

On a lower physical level, placement of devices within a facility should be done in a way that will maximize protection. In addition to "where", placement should be noted in the accreditation documentation in terms of doors, windows, and transmission media routing.

Physical routing of transmission media should indicate what transmission links, or parts of the links, are shielded, protected, and/or encrypted. Note that protection may vary with the security operating mode of a particular link. The way in which the media links are protected and accessed should also be addressed in the accreditation. For example, if a LAN trunk is routed under or near a well traveled road to provide better surveillance, detailed procedures would be required as to how, when, and why the trunk should be accessed for inspection or maintenance.

3. Network Management Appointments

In relation to accreditation of the generic LAN only one network manager would be needed. That person may be part of an internet management hierarchy if the LAN maintained an active gateway to such a system. In terms of security, the generic LAN requites a NSO and TASO. ADPSSOs are warranted where ever one of the connected computers is large enough to operate and support a standalone mainframe environment outside the NCC.

A situation could exist where there are a large number of terminals in addition to large numbers of PCs that are not accredited with the system, but are accredited on an individual basis to be used with the system. A separate TASO (or TASOs) for these PCs could promote better security for the system by ensuring all users understand and follow network procedures. In addition, such a person could better manage their unique and powerful capabilities. For instance, a site could have at least one TASO for each type of terminal approved for the network.

In addition to management of network components, accreditation documentation should include the role of network security management in all implementation and test plans.

4. Network Procedures

There are obvious procedures for the NCC and the network in general, that must be described in the accreditation package. They include escorts for maintenance personnel and other outsiders who have a temporary need to access the NCC or any secure network site. Other procedures include password control and issue, and audit procedures for regular review of network traffic. However, a gap exists in the guidance concerning control procedures for transfer of control to alternate control centers (AAC) when/if the NCC is destroyed or damaged. In the generic LAN (Figure 5.2) an alternate control center is not identified. Yet, if there was, there are no guidelines or requirements for transfer of system control in a distributed computing evironment. Thus, there is much flexibility in developing procedures for transferring control to another center. Plans and procedures developed for this kind of activity should be integrated into emergency plans and the COOP.

Basic accreditation considerations for procedures were brought out above in terms of crypto-key handling and disconnects. Besides standard key storage and handling procedures, key procedures could be used to simulate a disconnect on an encrypted network by simply not issuing the key to certain users for a designated period of time.

Another accreditation consideration is that system auditing software may or may not be acceptable for monitoring software or hardware disconnects. In addition, the fact that disconnects can or cannot be made at both ends of a transmission link should be noted. Thus, extra management procedures may be required for disconnect procedures in addition to the associated sanitization procedures.

5. Significant Applications

In terms of accreditation of a LAN, significant applications consist of software that handles/manipulates information or communications. In terms of the overall network, these types of applications need to be explained in terms of their compatibility and affect on overall network security and efficiency. Two examples are data base and message/mail sending applications. These applications are addressed later in the chapter under software.

6. Configuration/System Documents Required

Two important documents are the implementation plan and the ST&E plan. These and other major documents required for accreditation are mentioned in the beginning of the chapter.

7. Future Upgrade/Expansion

Assuming the generic LAN is accredited, any type of network upgrade or expansion will require the entire LAN configuration to be reaccredited. Reaccreditation is required when there is a:

1) Significant change to the physical structure of any facility containing network components. However, it would not apply to devices that were not accredited with the system unless the reaccredited process increased the sensitivity level of the entire network.

2) Major system hardware addition or replacement. Examples are addition/replacement of switches, encryption devices, interface devices, major large mainframe, and switching from coax to fiber optic cable.

3) Change in sensitivity processing level or operation mode category. Examples are SECRET to TOP SECRET and system high to controlled security operating mode.

In addition, even if an upgrade/expansion is not planned, a plan for implementation and review of additional security features is required for accreditation. Reference step 5 (requirement 5) in the analytical process outline presented in the beginning of the chapter.

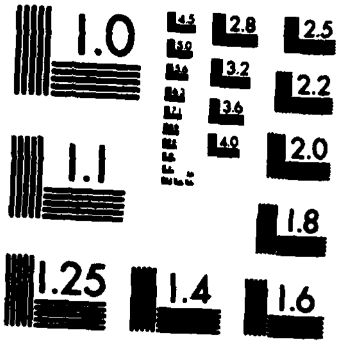
8. Waivers and Exceptions

Waivers and exceptions must be included in the accreditation documentation. If any part of a network cannot meet security guidance requirements, accreditation documentation must describe the circumstances and reasons that would impair operation and mission effectiveness. Plans must be included that describe and assure continuous progress toward full compliance. The accreditation authority cannot delegate authority to grant temporary exception, but may choose to submit it to the next higher accreditation level. All exceptions must be reviewed biennially to ensure that progress toward full compliance is made.

H. ADDITIONAL SYSTEM COMPONENT CONSIDERATIONS

1. ADP Hardware

Many of the basic device accreditation requirements are addressed above under system configuration considerations. In addition to the physical descriptions required by the FSP, hardware device descriptions should emphasize inherent security features and how they work with the network security features. Other areas [illegible]



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

emphasize are the affect of network security features on device performance, internal hardware control features, TEMPEST features, and/or low level emanation.

2. Terminals.

One point of interest is that terminals attached to the network more than 50% of the time must be accredited with the system. With the proliferation of PCs in the Army [Ref. 38: p. 4] this could mean great flexibility in a network context provided accreditation and approval for network connection is obtained for each PC connected to the generic LAN.

A powerful PC could perform many functions in a stand-alone mode, then connect to the LAN and communicate with other devices just long enough for the necessary data exchanges and distributed processing activity. Much could be accomplished by many powerful PCs operating in this manner even if they were connected to the LAN less than 50% of the time. This could be an advantage if network traffic is reduced, along with an increase in overall network processing, resulting from these PCs.

The major disadvantage would be the expense of accrediting each, or a group of terminals separately. Other considerations include development of access, connect, and disconnect procedures. These considerations would be further complicated in a controlled or multilevel mode because separate accreditation and procedures would be required for each security level. For example, if a PC was accredited for system high in a multilevel LAN, sanitization procedures would be required before switching to another security level. Conversely, a multilevel PC would not require sanitization and could be used anywhere in the multilevel LAN.

3. Software

Accreditation documentation must include major software (applications, executives, and utilities) with descriptions of the impact on network security features. General categories that should be included follow, however, there may be more depending on unique system requirements.

a. Protocols

The most significant gap in terms of network software is that no protocol security considerations exist in the guidance referenced. Communication software is also ignored by the guidance. Communications software implements the actual functional requirements for the transmission and reception of "coded" data for a device according to the rules of a specific protocol [Refs. 3,39: pp. 104,449-450]. A description of the protocol and associated communications software should be included in the accreditation documentation. Thus, protocol security analysis should be integrated with utility and operating system requirements in a way that will allow maximum overall network security. The relationship of protocols and system software was addressed in Chapter IV. Effects of encryption, audit trail, security features and major applications on the protocol, should also be included in accreditation documentation.

b. Data Manipulation Software

Data manipulation software generally falls under the data base management or data maintenance categories. The data base is one of the major computer-run resource today. Commonly, distributed systems distribute the storage among user locations. [Ref. 39: pp. 464-465] Thus, DBMS has important considerations in a network where information is accessed locally and remotely. System developers and managers must be sure it provides/supports audit trail and security functions. Data maintenance is another critical consideration because it is the access of data anywhere in the system via system software executives/utilities. Obviously operation and control of data manipulation software must be addressed in the accreditation documentation.

c. General System Software

As mentioned earlier, operating systems must provide as much internal control as possible. A unique situation exists in a network environment because each computing device may have different operating systems. Ideally, system software should make it easy to add new applications and security features throughout the network [Ref. 39: p. 457]. Similarly, each operating system should compliment network activities. Descriptions of all types of operating system, utility, and executive software should be in the accreditation documentation.

Software used for testing of the network and network security should also be described in accreditation documentation. [Ref. 39: p. 450]

I. TWO ALTERNATIVE EXAMPLES

Chapter IV presented considerations for the two operating mode extremes; system high and multilevel. Here, both operating mode examples will be taken one step further by looking at high level configuration alternatives for each.

1. Generic Configuration - System High or Dedicated Design

There is not much change in terms of the original configuration for the system high or dedicated operating modes. The security issues concerning the configuration at a "high level" design stage include determining if it will be a total PDS, whether some or all lines will be encrypted, and what buildings and/or equipment should be shielded. In addition, combinations of encryption, shielding, and physical protection can be considered. Figure 5.2 illustrates an unchanged generic configuration; in terms of a PDS, any part of this (Figure 5.2) could be encrypted, shielded, or protected. For example, cryptography equipment can be put at each end of major trunk lines to encrypt a particular link, without affecting the original configuration. Compare Figure 5.2 to Figure 5.3 If this encrypted configuration (Figure 5.3) was implemented between buildings, it could be configured as depicted in Figure 5.4 Given the major trunks are protected by encryption, each individual building, or room(s) containing network hardware, would have to be shielded. Another alternative would be to shield all the hardware components. In contrast, Figure 5.3 illustrates the generic configuration totally encrypted. Only the trunk lines are encrypted in Figure 5.4

2. Multilevel Example - High-level Design

The multilevel configuration takes on a whole new shape in contrast to the generic configuration. The reason is that the multilevel configuration example does not base system control on trusted sophisticated operating system mechanisms like security kernels [Ref. 37: p. 283]. The "kernel" is the nucleus of the operating system kept in main memory while the computer is operating, and consists of routines that handle input/output (I/O), scheduling, and other basic system functions [Ref. 3: pp. 209,263]. A security kernel consists of the software, firmware, and hardware in a trusted computing device that can be protected from modification, mediate all accesses, and be verifiable [Ref. 21: pp. 112,113]. However, the major element in this example is the trusted interface unit (TIU).

a. The Trusted Interface Unit (TIU)

In short, a TIU enables a user to be at just a single security operating mode level, or a range of security levels (multilevel). The TIU is a device that checks and enforces control labels/fields on each information packet transmitted to it. A packet is a group of bits that make up all or part of the message to be transmitted [Ref. 3: pp. 276-277]. Messages longer than the network's packet size are broken into smaller sections, and consequently are distributed over more than one packet. Control

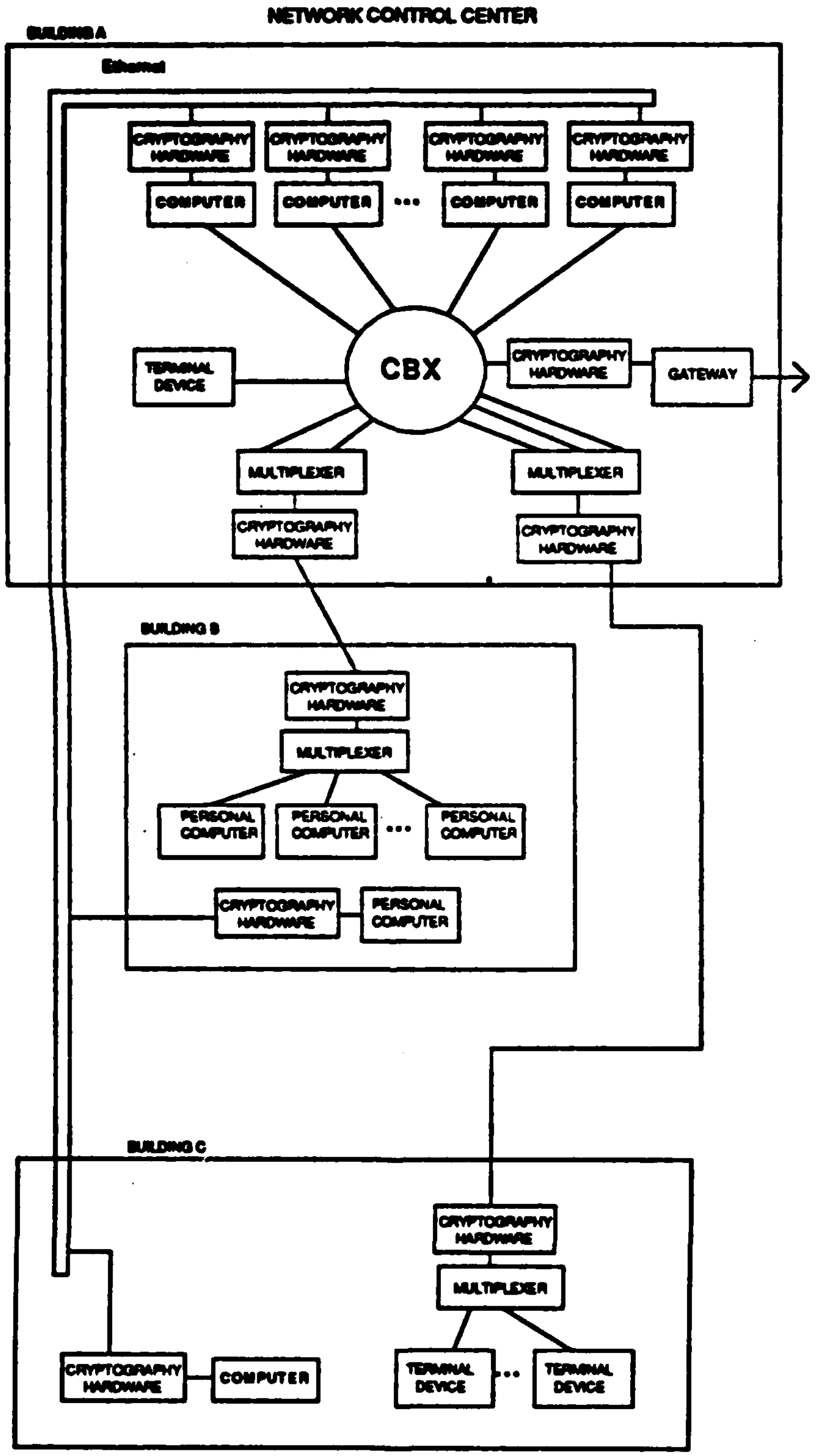


Figure 5.4 The Gerneric Configuration Between Buildings.

labels and fields identify information required for routing the packet through the network to its ultimate destination. Packets not meeting requirements cannot pass through the TIU. All computers transmitting to the TIU are trusted to receive and send packets at the security level they are approved for.

Each individual TIU can be set to monitor a single security level or multiple levels. Each level of security traffic is isolated from the other. Consequently, single level TIUs are restricted to one and only one level. However, variable level TIUs are adjusted by electrically linked terminal switches or keyboard keys. The range of adjustments correspond to the approved security levels for that particular TIU and terminal. Multilevel TIUs must contain fully trusted software, but a network can operate in a multilevel mode using only single and variable level TIUs. See Figure 5.5 [Ref. 37: pp. 281-285]

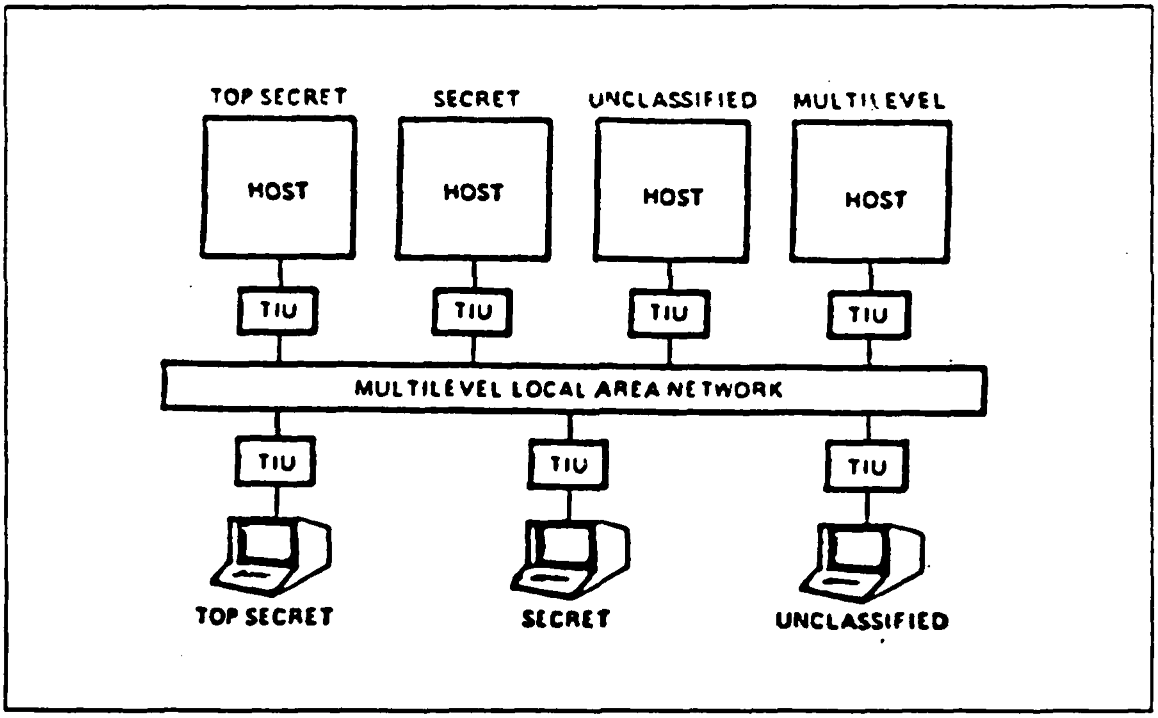


Figure 5.5 Simple Multilevel LAN.

b. The Configuration

The overall design strategy is intended to be easily implemented with "off-the-shelf" hardware and protocols. In reality the TIU design strategy creates one subnetwork for each security sensitivity level. Each subnetwork is protected at the system high level designated for that subnetwork. Bridges connect each subnetwork to form the multilevel network. See Figure 5.6 for a detailed example of the subnetwork configuration. [Ref. 37: pp. 281-286]

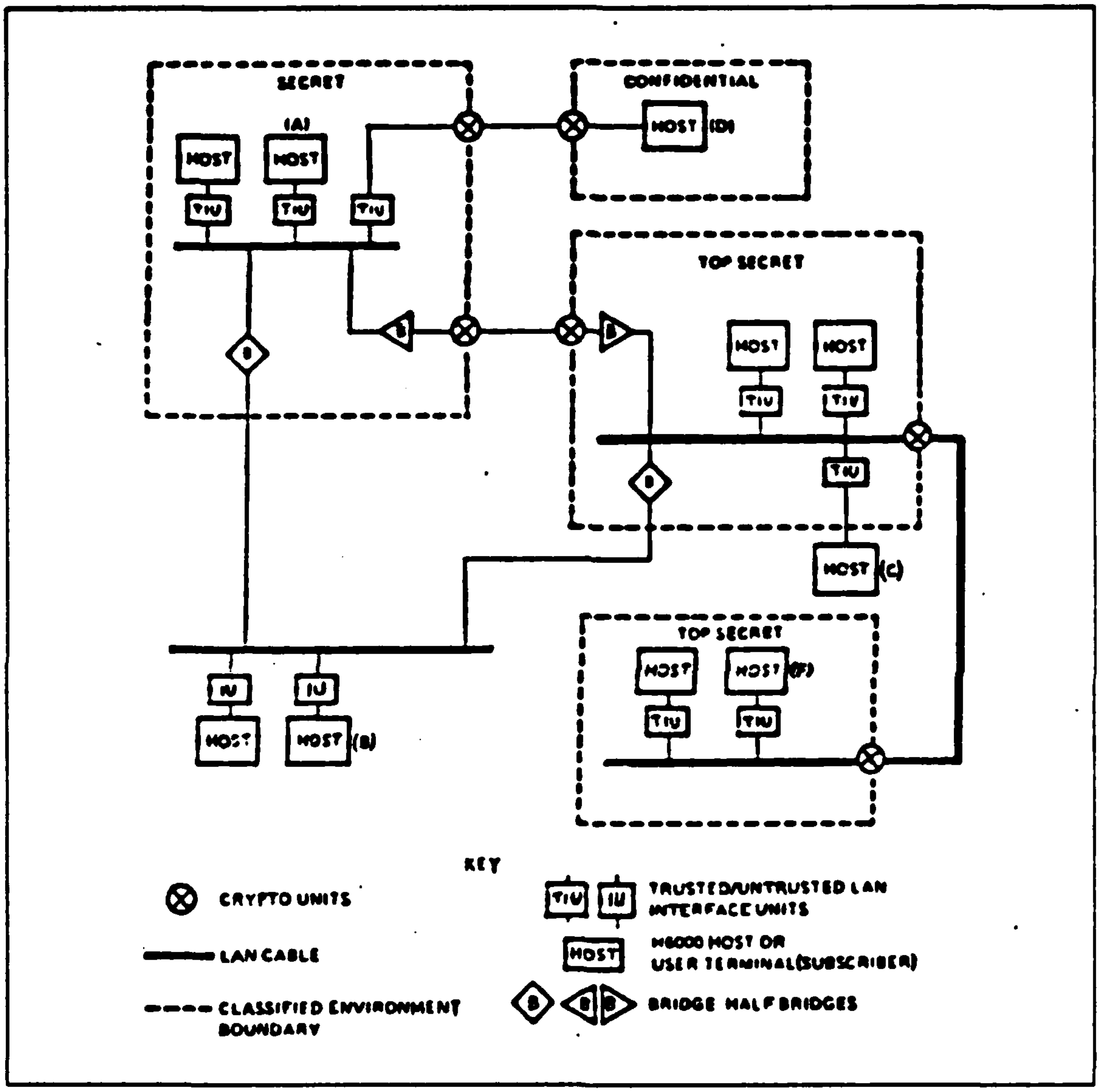


Figure 5.6 Multilevel Subnetwork Configuration.

The definition of a bridge in the TIU network varies slightly from the Chapter II definition. Like the Chapter II definition, the TIU-based definition states that identical protocols are used to route packets between LAN subnetworks. But in addition, the TIU-base definition requires that the bridge perform security checks to prevent sensitive information from flowing from a higher to a lower level subnetwork. The bridge functions are transparent to the TIUs and other devices. What's more, the bridge only checks security levels between the two networks it is connected to. In doing this, it does not verify the level of the packet in terms of the source it is from, or subnetwork destination. Note in Figure 5.6 that split bridges are used to identify areas where encryption might be implemented; for instance between two buildings. [Ref. 37: pp. 282-287]

This design example is based on the Ethernet protocol. The concept could be applied to the same environment as the generic LAN, but the overall configuration would be drastically changed. A possible high level configuration is illustrated in Figure 5.7. Note the difference between Figure 5.7 and the generic configuration in Figure 5.2. [Ref. 37: p. 283]

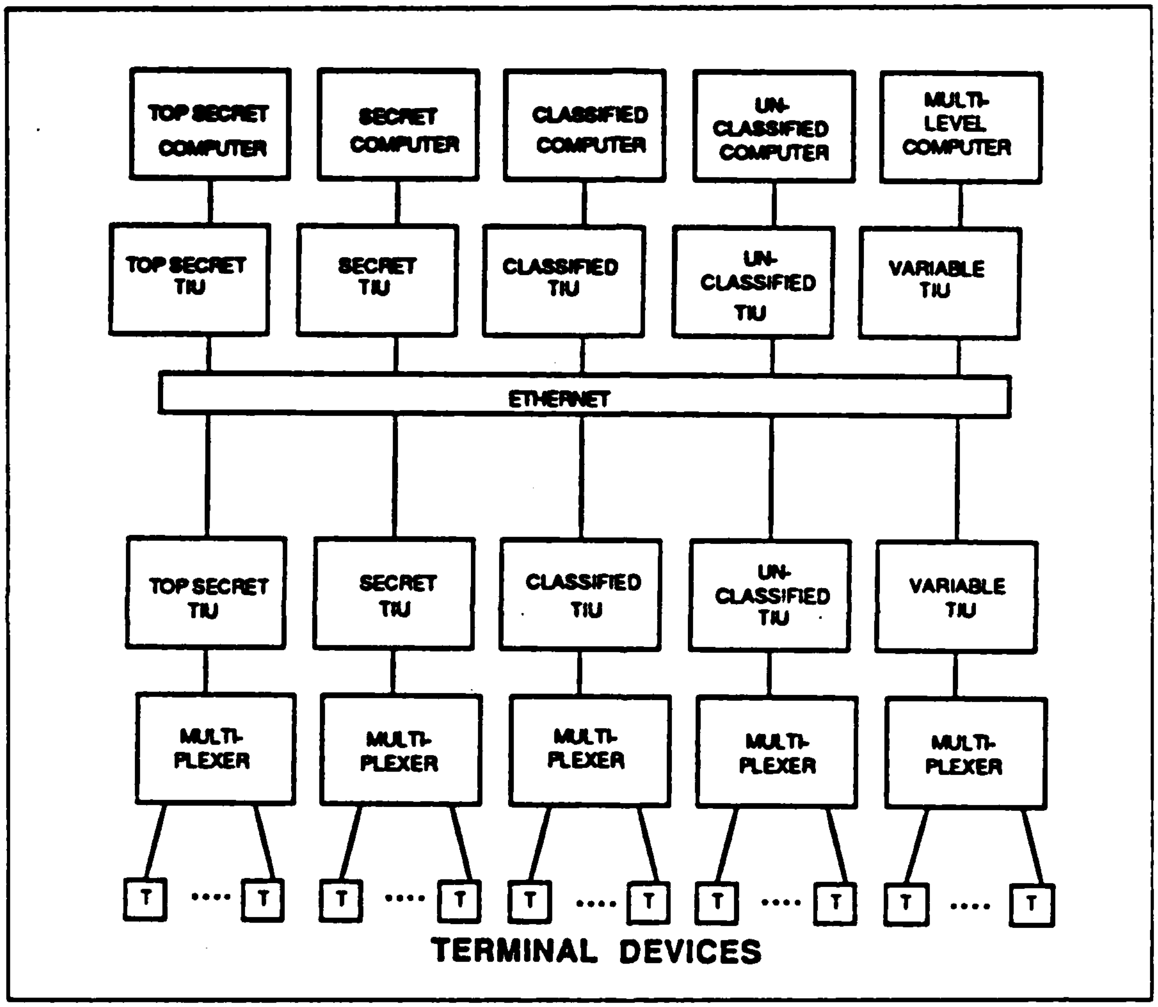


Figure 5.7 Multilevel LAN - High Level Configuration.

VI. CONCLUSIONS AND RECOMMENDATIONS

A LAN is a general-purpose local network that is normally used for minicomputers, microcomputers, and terminals, but can support many other devices. LAN applications and numbers are growing. One reason is that they provide flexibility and resource sharing of limited hardware resources. Unfortunately their distributed nature increases their vulnerability in terms of securing the information they contain. Thus technical computer security guidance must be applied effectively to LAN configurations. [Refs. 13,1,4,40]

In general, application of technical security guidance requires that the vulnerable LAN areas must be identified and categorized as risk factors early in the system development. Next, these factors must be quantified so the overall system sensitivity can be determined, which in turn allows identification of security requirements for the system. [Refs. 13,40]

A summary of the thesis with conclusions follows. Then, some general recommendations are presented.

A. SUMMARY AND CONCLUSIONS

1. Sensitivity

Requirements identified in Chapter III indicate that sensitivity is determined by the importance of the information processed to the overall Army mission, a need-to-know, and unique system features or applications that warrant protection. The sensitivity determination controls the type of information and thus the databases which could be tied into the network or LAN. Sensitive information can range from mission oriented data to non-mission oriented data like large dollar volume inventories and personnel data covered by the Privacy Act of 1974.

The need-to-know requires a "need-to-protect" information contained in the system. Protection determines who will access the network and how they will do it, as well as the physical protection of hardware components. The protection (i.e. security) features must be cost effective and production effective. The first step to implementing efficient security features is to correctly select the maximum sensitivity level required for the network based on information presented in Chapters IV and V, and then select an adaptable security operating mode.

All guidance referenced stressed that sensitivity of data be based on a "need-to-know" which is a valid approved need, based on damage to national security and required for performance of duties [Ref. 20: p. 10]. Army sensitivity designations are CRITICALLY SENSITIVE, HIGHLY SENSITIVE, SENSITIVE, and NONSENSITIVE. These designation categories have the same requirements as the "Orange Book" but different labels. [Refs. 13,21]

Sensitivity determinations are also affected by compilation. Compilation of data occurs when certain types of data/information and large dollar volume assets are combined to yield a higher security classification than they would normally be assigned individually [Ref. 20: p. 11]. There is great potential for compilation in a network because information can be extracted from distributed locations and combined or "compiled".

As mentioned above, the operating mode classification is dependent on the designated network sensitivity level. Security operation modes that apply to all types of systems are dedicated, system high, controlled, and multilevel. The more sensitivity levels and access flexibility, the more complicated the system, given today's guidance and technology. For instance, the dedicated mode is the least complicated to administer, but only provides one level of security. Also, dedicated operating mode requirements could be applied to any network configuration. Conversely, the multilevel mode is more complicated to administer (with current technology), but provides simultaneous operation/processing of more than one security classification on the same network. In addition, the multilevel mode may not be applied to all configurations; an example was presented at the end of Chapter V. [Ref. 13]

It should be noted that DOD contractors are limited to dedicated, system high, controlled and concurrent processing modes. The multilevel mode is not addressed for contractors, but concurrent storage and processing of multiple levels of information is approved for contractor run and approved systems [Ref. 36: pp. 173-175,181-182]. Generally, system high protection is required for all components.

2. Configuration

LANs have emerged as a practical way to turn mainframe environments into distributed networks [Ref. 9: p. 69]. The generic configuration in the thesis uses a combination of a bus and star topology to illustrate a LAN. The design is a practical administrative network configuration. An Ethernet bus is used to handle host traffic while the CBX forms the star configuration used to control user device traffic.

Expansion possibilities for the generic LAN include multiple gateways to other LANs and wide area networks, and installation of multiple switching locations. User applications could be expanded into expert systems, graphics, and relational data base systems.

It is beyond the scope of the thesis to go into specific security cost effectiveness analysis of configurations and components. The purpose is to give the reader a better feel for security boundaries in an Army LAN.

3. The Security Goal

The goal is to design and implement a secure system that has little impact on responsiveness and efficiency of the network components, as well as the overall network. To do this, system vulnerabilities and the impact of system security features on network performance must be limited.

Vulnerabilities must be identified so a sensitivity level is established early, and in the design stages of development. Vulnerabilities must be limited to prevent penetration of network security. In addition, the access threat is growing, especially in terms of communication taps and microwave signal interception from equipment emanations. Considerations like accounting and audit trails, individual accountability, and data integrity must be included along with physical security. Once a security operation mode is chosen, security requirements for each network component can be identified. [Ref. 1,5]

Impact of security features must be a major concern of system developers, because network components usually do not have inherent security features. For instance, in Ethernet, encryption and general security is the responsibility of the "end-user processes." [Ref. 18: p. 54] When security features are combined with a security processing mode a LAN configuration can take on a very different appearance. Again, an example of the impact of security on a network configuration was illustrated in Chapter V. It showed that a multilevel system configuration versus system high or dedicated mode configuration can be very different, in terms of the resulting configuration structure and it's associated hardware components, like the trusted interface unit (TIU).

The multilevel operating mode was identified as the most complicated and therefore the hardest mode to secure and maintain. A particular multilevel operating system may not be approved for all applications at a given classification level. Moreover, the "system effect" may reduce over-all multilevel sensitivity performance.

This is because the operating system is the main component in a true multilevel system, although a multilevel environment can be achieved with conventional hardware and software.

In contrast to true multilevel operating system requirements, system high and dedicated modes do not require memory partitioning or other memory unique control functions in the multilevel sense. System high and dedicated modes do require special procedures (sanitization, disconnects, approval, etc.) to move to a higher or lower security operating mode.

In the final analysis a system must meet user requirements and be robust and responsive as well as be secure. Again, security features and the designated network operating mode can have a major impact on the design and operation of a network. The ultimate goal is to have all security features and procedures totally transparent to the users. Lack of network security guidance allows flexibility in pursuit of this goal, but at the same time interpretation and accreditation may cause frustration for the developer.

Additionally, this goal may never be fully realized in the real world of Army ADP and network system application. The reader should recognize that possible problems with development, system acquisition, time constraints, resource/money constraints, and general implementation, to mention a few, can have a significant impact on the resulting system and it's security features. Nevertheless, it is beyond the scope of this thesis to address or speculate how these factors may affect network security implementation and accreditation. At least, the accreditation process forces the system sponsor and developers to address security in some way.

4. Accreditation

In the rush to modernize ADP systems and continually update software, new ideas for regulations and system protection have been sidetracked [Ref. 2: p.3]. There is almost nothing in the guidance reviewed for this thesis that pertains to "LANs" specifically, and very little in terms of direct references to "networks" in general. But, the guidance reviewed does address ADP security topics that relate to general LAN/network components. AR 380-380 is used as the focus for all other guidance reviewed for this thesis because it is currently the number one guidance for ADP security in the Army.

The guidance does not address LAN security in great detail. Various telecommunications, ADP, and ATS components are all used to establish LANs. In addition to interpretation, the developer must derive most LAN requirements himself/herself because only a few checklists reference networks directly [Ref. 24,25]. Any LAN is subject to ATS and general ADP requirements, even if it is purely an administrative system, because LANs consist of ADP components and always include telecommunications [Ref. 13: pp. 9,31]. Consequently network security guidance for accreditation of sensitive systems is obtained as a result of a synergistic effect from complying with ADP, ATS, and other types of guidance. Conversely, nonsensitive systems don't require accreditation. [Ref. 13]

In terms of system security and eventual accreditation, many network component and topic areas are not covered or inadequately covered. However, there are many regulations that apply to network components. For instance, all sensitivity designations and operating modes apply to networks, including compilation. Site security must equal the requirements for the highest level of information processed at that site. All network components must be protected with shielding, encryption, and the appropriate physical security. Before an ADP system, terminal/device, or a network can access or interface a specific ADP network, the ADP system, device, etc., must meet approval of the DOD component, and the agency operating the network [Ref. 22: p. 20]. Any computer (micro, mainframe, etc.) collocated or connected to the network more than 50% of the time must be accredited with the system [Ref. 13: p. 9]. A final noteworthy example is that privately owned computers cannot be used in a sensitive network environment or any type of remote connection to a sensitive mainframe computer. [Ref. 13: p. 10]

In contrast to regulations that apply, regulations that do not apply take on two forms - waviers and exceptions. An exception is a case to which a rule does not apply [Ref. 31: p. 432]. Exceptions will depend on characteristics unique to the system, which may include the sensitivity of the information, the characteristics of approved ADP equipment, the characteristics of substituted equipment, the results of risk analysis, and the organizations involved. In short, exceptions may result because security solutions are not feasible. [Refs. 13,32,20]. A wavier is a privilege to intentionally abandon a known requirement [Ref. 31: p. 1325]. The intent is to provide an opportunity to simultaneously fix and operate the network; not an excuse to ignore security discrepancies. A wavier is used when complying with guidance would impair operation and mission effectiveness. Note that continuous progress must be made toward full guidance compliance and that just one critical component could require a wavier for the entire system.

In addition to guidance that does and does not apply to networks, there are outdated regulations and network topics that are not covered. Guidance has a mainframe flavor, for instance, there are references to punched cards. In contrast, there are few direct literal references to networks. Mainframes still exist, but networks and their applications are increasing, especially in administrative applications [Ref. 41]. Thus, specific network and LAN guidance would be valuable.

The thesis also looked at network security topic areas not covered by the guidance. Much interpretation from ADP and ATS guidance is noted throughout the thesis. Notable topics not covered include protocols and the impact of PC's on security. The only specific fact is that PCs must be accredited with the system if connected for more than 50% of the time [Ref. 13: p. 9].

Even though the guidance reviewed does not literally address, and in some cases does not apply to LANs, there still is enough guidance to prepare a LAN for accreditation. The accreditation process consists of designing a system, documenting its operation and security features as required by the guidance, and preparing the documentation for review by a designated approval authority. It includes a series of reviews and meetings and ends with the designated approval authorities written approval. More risk requires higher command/management levels of responsibility and awareness, because the approval level is raised to the next higher authority if accreditation requirements can't be met at a given level.

5. Physical Protection

There are no gaps in environmental and physical security requirements; all physical requirements apply to LANs. One method of physical protection is the protected distribution system (PDS). A PDS is an approved telecommunications system that has the required physical and electronic safeguards for safe transmission of unencrypted sensitive information. [Ref. 13: p. 76]

Physical protection varies with emanation protection (TEMPEST) to a certain degree. It is not unreasonable to require encryption or shielding, or even have a combination of both. Consequently, a PDS could have either shielding or be encrypted, or be a combination of both. Price/flexibility trade offs must be determined by the organization developing the network to determine which alternative is most affordable, and will allow expansion, for the desired level of protection.

The Facility Security Profile (FSP) is one of many documents required for accreditation. It is the physical security description of all facilities containing network hardware and includes a list of hardware, hardware locations and relationships, and general functional operation of the network environment.

In general, physical security corresponds to the highest sensitivity level processed at the network site. Power supply facilities for the network must be physically protected at the system high too, because any ADP system or network requires electricity to operate. Obviously a network and it's information is useless without a power supply. Moreover, any security features supported by the same power source would be useless. Also, interface requirements parallel standard ADP or telecommunications requirements depending on the device characteristics.

6. Network Access

Security procedures are required for internet and intranet gateways and other interface devices. The procedures should be the result of an agreement by all networks involved. Audit procedures and password controls in the form of flexible network audit and monitoring features, should provide operators and managers easy tracking of data as it is routed through the network, and users on the system. Audit file information should be limited to network management.

In terms of physical controls, personnel access to network sites can be limited by physical barriers, security identification badges, TV monitors, and visitor escorts. Moreover, access can be limited during emergencies. Emergency procedures for start-up shut-down, and system failure must be planned because the network is especially vulnerable during unscheduled termination of operations [Ref. 13: p. 24-25]. In addition, physical access procedures must consider the protection of system documentation and media must be protected at system high for the location (this includes disks, tape, etc.). Nonetheless, if the system is not multilevel approved, everything (disks, tape, data, etc.) that goes into the system comes out, and is controlled, at system high. This includes any input that has a lower system classification level. For example, consider an unclassified floppy disk brought into and used in a network control center that operates at the SECRET level in a system high mode. From that point on the floppy must be labeled and handled as SECRET.

Encryption and/or shielding is required to secure network devices against access via emanations. Isolation transformers and powerline filters are used to prevent signal emanations via the power source and its components. In addition to normal ADP/ATS encryption devices and software, there is a lot of encryption software available for PCs [Ref. 38: p. 4]. Major encryption considerations include extra procedures for maintaining signal synchronization throughout the network, and crypto-key distribution.

Given the sensitivity level of the network site, ADP hardware security features require isolation of users in regard to the designated security level for internal controls. Various external device access controls like locking mechanisms, keys, electronic cards etc., may be external device requirements.

7. Software

The software guidance is ADP oriented; there was no mention of network protocols. Thus, general statements about utility, application, and operating system software were presented in terms of how they must work with a protocol to maintain a secure network operating environment. In short, a protocol is a set of rules, that transform into requirements and specifications for the executive, utility, and applications software that control network interaction.

Use of software security packages should be based on cost versus level of security protection provided. In other words, it should be analyzed to verify that it does work as the vendor claims. Moreover, classified data cannot be protected by commercial software alone, so proper management procedures should accompany it's use. For instance, issue of passwords the particular commercial software may require.

8. *Miscellaneous Network Management Considerations*

Management can best control network security by taking advantage of all the system security features. Continuous controls, like audit and monitoring hardware and software, can be of great value because networks are inherently unsecure due to their distributed nature. But before network management relies on security features, the features should be verified and tested. When determining the security mode and actual network components, security system verification should be a major consideration. For example, verification of "true" multilevel network security is in it's infancy. This may or may not impact a given implementation effort, however it should at least be a consideration.

Given the extra procedures often required for security features and the distributed nature of LANs, it may be wise to give more security responsibility to the users. In any application, pure distributed data management involves the increased sharing of responsibilities (with users) for managing functions of processing, movement, and storage of information. [Ref. 7: pp. 6-8]

B. RECOMMENDATIONS

1. General Protection of the Generic Configuration

Security considerations and requirements should be identified as early as possible in the design phase of the network. Chapter V showed how different configurations can result from different security needs. Guidance also stresses early application of security features to the overall network design. System security impact should be analyzed in terms of procedures, physical requirements (fences, surveillance, etc.) cryptography, software, training and management control and monitoring. Moreover, configuration considerations must include responsibilities of network security and management personnel. At a minimum a network should have a network manager, a network security officer (NSO), and at least one terminal area security officer (TASO) during the design phase as well as for implementation and operation.

Given that network guidance is practically non-existant in the guidance documents, general guidance pertaining to individual LAN components should be followed. For instance, ADP guidance for network computers and ATS guidance for network transmission media.

Internet access should be tightly controlled and limited as much as possible, preferably using only one tightly controlled gateway. Dial-up capability should be eliminated in networks processing sensitive information, because multiple entry alternatives provide many opportunities for unauthorized access.

In addition, security procedures should provide tight control of ADP storage media, especially removeable floppy disks; possibly using classified document control procedures. Floppy disks are easy to load, copy, conceal, and steal.

If encryption is used throughout most of the LAN, encryption keys could be used to simulate a software disconnect where certain components could not be approved for a temporary higher classification operating mode, and special procedures are developed.

2. Important Guidance to Reference

In general, this thesis should be read for an overview, followed by a review of AR 380-380, by anyone about to be involved in LAN development. AR 380-380 is the focus because it is the current, major document dealing with Army automation security guidance. In addition, the Orange Book will provide more background on sensitivity designations - the key to ultimate network security requirements. Remember a need-to-know and need-to-protect determine the sensitivity which in turn drives the security requirements.

Note that some guidance encourages common standardized connections of hardware to promote Army interoperability goals. In addition, security features should be part of any network interoperability plans and goals. [Refs. 13,28,29]

A unique point in one regulation states that COMSEC testing is currently done on request. This should be mandatory for all networks so emanation control can be verified. [Ref. 30: pp. 4-5].

In terms of organizational position and assignments of personnel, AR 380-380 provides comments on separate assignment of responsibility for physical and non-physical (software security, audits, etc.) security functions. Sensitive personnel positions are determined by a need-to-know and the security operating mode. [Ref. 13: pp. 6-7]

3. Future Research

One major area not covered by guidance is the network impact and specific security of PCs. Desk top power in the form of PCs and other microprocessors can now do many of the tasks that previously were only performed on mainframes and minicomputers. This is an obvious threat when you consider the ease with which a PC is moved and connected to a network or another device [Ref. 38: p. 4]. Much research should be done in this area.

Even though ATSs were addressed, no protocol security guidance existed in the same regulation. Obviously, protocols are another major LAN component that needs be analyzed in terms of Army security guidance and requirements. [Ref. 13]

Many areas were not covered due to the limited scope of the thesis. First, personnel security was not addressed, yet personnel security considerations should be one of the most important. Personnel guidance can be found in AR 380-380. Furthermore the thesis did not cover all aspects and details of accreditation or all aspects and details of contractor security. In addition, the following LAN topics and components are suggested for further security analysis and research.

- Operating systems.
- Risk management.
- Research into current regulations being drafted as opposed to what currently applies.
- System sanitization.
- Trusted and/or smart interface units.
- Distributed data storage procedures.

Suggestions for possible future guidance research areas are listed below.

- More detailed network security analysis into one or more of the security operating mode designations, possibly using this thesis and expanding it in detail.
- Multilevel trends in security technology and their application to networks.
- Distributed processing security.
- Encryption of data over a network.
- Apply this thesis to a specific network and point out specific deficiencies in guidance.
- Explore more aspects of the accreditation process in more detail.
- Development of an accreditation plan or regulation document that covers detailed requirements for ADP systems, ATSs, and networks.
- Develop detailed guidance for LANs. Use this thesis as a primer and background for developing such guidance.
- Develop security guidance for distributed network control.

C. FINAL COMMENTS

New technology developments should be used when possible to enhance the robustness, responsiveness and efficiency of any computer network. User resource limitations require that the network yields cost effective operation and installation. Nonetheless, military requirements for protection of sensitive information processing may prove to be a challenge in terms of network operation and performance. Performance factors should not degrade the level of protection of the system [Ref. 22: p. 2]. Conversely, the security requirements should not degrade the network to the point of uselessness. Consequently, military guidance interpretation can be difficult, especially when/if it does not keep up with technology.

APPENDIX
SECURITY GUIDANCE SUMMARIES

1. INTRODUCTION

Army Regulation 380-380 (AR 380-380) is covered in more detail than the other regulations because it is the one regulation specifically dedicated to automation security.

2. REGULATION/GUIDANCE SUMMARIES

a. ARMY REGULATION 380-380: Automation Security, 8 MAR 85

1. Purpose.

AR 380-380 was developed to provide a minimum standard for all non-conflicting areas and areas where higher guidance does not exist. Thus, it is not intended to duplicate higher guidance. However, the more stringent requirement will take precedence when there is a conflict. Conflicts between agencies are possible because many other agencies govern certain Army ADP systems. Some examples are the Defense Intelligence Agency (DIA), National Security Agency (NSA), and Defense Communications Agency (DCA).

In general this regulation is designed to address automation security and allow accreditation authorities and individual commanders to apply stricter controls and procedures, if necessary. [Ref. 13: p. 3]

Another major function is to describe the Army Automation Security Program (AASP) which consists of ADP system security and automation resource subject areas. Automated data processing (ADP) system security includes: security management, software security, hardware security, procedural security, communications security, personnel security, document security, physical and environmental security. Automation resources include: all computer equipment, remote terminals and peripherals, programs, data, associated documentation, contractual services, personnel, supplies, facilities, intelligent terminals, minicomputers, microprocessors, and automated office systems.

2. *General summary.*

The following AR 380-380 chapter summaries identify important items related to LAN security, and network or security related ADP.

(1) *Chapter 1. Overview.* This chapter is an overview of basic security guidance covered in AR 380-380. After the general purpose (explained above), basic ADP security responsibilities from the highest to the lowest levels are explained. Positions identified that apply to LAN security are the terminal area security officer (TASO), network manager, and network security officer (NSO). The TASO is "appointed for the remote terminal(s) and interface devices(s) connected with a host computer." A network manager is "assigned when two or more automated systems join to participate in networked operations. He or she will prescribe security mode and requirements, protocols, and standards for the network." A NSO is "appointed for each network processing sensitive defense information. Note that NSO responsibilities include network access and connectivity control; security impact evaluations of network changes and interfaces with other networks; and maintaining a network security profile. [Ref. 13: pp. 3-5]

Major policies include that all computer facilities and operations will be designated either as critically sensitive, highly sensitive, sensitive, or nonsensitive, and that system security applied at the beginning of the design is more cost effective in the long run. AR 18-1, AR 105-22, AR 1000-1, and DAR MISC Pub 28-24 are cited as references. Additionally, network security measures must be established before internetting operations begin (between both/all networks). Any ADP system, sensitive or higher, must pass all accreditation processes. [Ref. 13: pp. 5-6].

Minimum Department of Defense (DoD) requirements are identified and include individual accountability, physical and environmental control, system stability, data integrity, system reliability, communications links, and classified and unclassified national security information. [Ref. 13: p. 6]

General ADP, information sensitivity determination, and sensitivity levels, can be changed to more restricted limits if an accreditation authority determines that the sensitivity designations are too broad.

Conversely, an accreditation authority can move to one sensitivity level lower than prescribed, if the following conditions are met: the volume of sensitive information processed is low, the sensitive information is always confined to a specific area, adequate and continuous protection is exercised at each sensitivity level, and personnel are properly cleared. In addition, all sensitive personnel positions must be formally defined.

The four basic levels of security are Critically Sensitive (CS), Highly Sensitive (HS), Sensitive, and Nonsensitive. The CS level is broken down into sublevels: Level 1 (CS1) for sensitive compartmented information (SCI) or Single Integrated Operational Plan--Extremely Sensitive Information (SIOP-ESI); Level 2 (CS2) for TOP SECRET; Level 3 for SECRET/CONFIDENTIAL. [Ref. 13: p. 6]

Operational service modes for the purpose of this regulation are identified as local, remote batch, remote interactive, and networked. Local is the least complicated service mode, remote batch and remote interactive are progressively more complicated, with networked considered the most complicated. The more complex the operational service mode, the more vulnerable it becomes; this is one key factor in determining the vulnerability and risk of the system.

In short, access control topics are concerned with a need to know using only the resources needed and is dependent on security processing modes and restrictions. Also, requirements, characteristics, and basic features for the multilevel, controlled, system high, and dedicated security processing modes are addressed along with periods processing. [Ref. 13: pp. 7-8]

If intelligent terminals, minicomputers, and microprocessors are collocated or connected to another automated system, more than 50% of the time, the terminals, etc., must be accredited with that system. This assumes a LAN or ADP system requires accreditation. In terms of automated administrative systems, any system attached to a sensitive system requires accreditation. Word processing work stations are considered remote terminals and should be part of the accreditation and risk management documentation. [Ref. 13: pp. 9-10]

Additionally, privately owned computers are discouraged. They must comply with AR 380-380 and accreditation requirements, and be used in a stand alone configuration. All information processed becomes property of the Army organization in which the computer is used. [Ref. 13: p. 10]

The first chapter of AR 380-380 also addresses accreditation authority designation requirements, and waivers and exceptions of security requirements.

(2) *Chapter 2. U.S. Army Automation Security Program (AASP).* The U.S. AASP was developed to achieve the most economical and effective security for Army ADP systems. Some management responsibilities include "ensuring that new systems, or major revisions of existing systems include automation and communications security in their design"; and "that construction of new automation facilities conforms with the security requirements of this regulation." [Ref. 13: p. 10]

Other topics covered relating to AASP are implementation at the Headquarters, Department of the Army (HQDA) and major Army command, post/installation-level, and data processing activity (DPA). In addition, the U.S. Army Automated Data Processing Systems Security Enhancement Program (ADPSSEP) and the DoD Security Evaluation Center are addressed. [Ref. 13: pp. 10-11]

Network processing and security implementation includes [Ref. 13: p. 11]:

- Ensuring "the establishment of minimum standards for the security and operation of the network and ensure adherence";
- Ensuring implementation of a system wide network risk management program and network security procedures;
- "Periodic review of network security";
- Providing configuration management (software and hardware), and making sure software and hardware is tested and approved before use.

(3) *Chapter 3. Physical and Environmental Security.* "This chapter provides standards and criteria for physical security measures required to safeguard fixed and mobile data processing activities." Physical security must be included in a balanced automation security program. The objectives include: safeguard personnel; prevent unauthorized access; safeguard against espionage, sabotage, damage, & theft; reduce exposure to threats that disrupt service. Note - only limited aspects of Chapter 3 are addressed in the thesis.

Physical security principles covered include barriers, procedures, construction standards, and physical access controls. Areas addressed in Chapter 3 apply to remote terminals, nodes, peripherals as well as the central computer complex. [Ref. 13: pp. 12-16]

(4) *Chapter 4. Personnel Security.* Personnel security and surety was not included in the scope of the thesis. Nonetheless, Chapter 4 covers general personnel policy, implementation of the Personnel security and Surety Program (PSSP), initial evaluation and screening, selection and retention criteria, personnel security

investigations, local national employees, security briefing and debriefing, and PSSP maintenance. [Ref. 13: pp. 16-18]

(5) *Chapter 5. Communications Security.* In terms of LAN security, communications security (COMSEC) and terminal access are two important topics covered in this chapter. Army COMSEC "policy requires that all record telecommunications will be secured by either encryption in approved cryptographic systems or protected distribution systems (PDSs)". In addition "all circuits used to interconnect remotely located components of Army automation systems or networks will be provided COMSEC protection under the provision of AR 530-2." By consequence, methods for achieving COMSEC are addressed also. Topics relating to terminal access include locking and unlocking, and physical and logical disconnects.

Other topics covered in Chapter 3 are system password generation and control, and communications security planning. [Ref. 13: pp. 18-19]

(6) *Chapter 6.* The importance of hardware security is stressed in Chapter 6. In general, areas covered include guidance on hardware security policy, desirable hardware security features, and considerations outside the CONUS. In relation to LANs, desirable HW security features are hardware/firmware that isolate users from each other and constantly monitor the system to identify terminals and users logged into the system. [Ref. 13: pp. 19-20]

(7) *Chapter 7. Software Security.* For the purpose of AR 380-380 software is broken down into general purpose, executive, utility, and software categories. Areas addressed are general software security guidance, operating system security features, data base management system (DBMS) features, and software security packages. It should be noted that "classified data will not be protected solely by commercial software. In addition, classified data processing requirements will not be used as the sole justification for acquisition of such software."

Areas of Chapter 7 that apply to LAN security include items that address remote access, identification of remote terminals, and control of remote terminals via software. Also, shared data bases are addressed. [Ref. 13: pp. 20-22]

(8) *Chapter 8. Procedural Security.* "The purpose of this chapter is to prescribe procedures and techniques which can be applied to improve control, reduce risks, and counter inherent vulnerabilities of a data processing activity (DPA) or" an automated teleprocessing system (ATS). Areas covered in this chapter include:

- Management considerations.
- Software design.

- Start-up, shutdown, and system failure procedures.
- Control of over-the-counter batch jobs.
- Control of teleprocessing systems jobs.
- Continuity of Operations Plan (COOP).
- Accountability procedures.
- Security of ADP media.

Topics that relate to LAN security include facilities configuration management; system start-up, shutdown, and failure affects on remote devices; and control of ATS jobs. Note that requirements pertaining to ATS jobs are mandatory for all new Army systems. [Ref. 13: pp. 22-29]

(9) *Chapter 9. Risk Management.* Risk management must be a responsibility of each command "because each computer site and operating environment is unique, there are no standard remedies or checklists which can be applied. . . Management must identify the resources to be protected and analyze the risk of espionage, sabotage, damage, and theft to determine the minimum level of protection needed." Generally the objective of risk management is to obtain safeguards against unauthorized access and manipulation of information. Note that Appendix O addresses procedures for identifying vulnerability and penetration areas. Areas covered in Chapter 9 include [Ref. 13: pp. 29-30]:

- Risk Management Methodology.
- Risk Assessment.
- Management decision.
- Control implementation.
- Effectiveness review.
- Implementation.

(10) *Chapter 10. Accreditation.* Accreditation is addressed in Chapter V of the thesis.

(11) *Chapter 11. Automated telecommunication systems (ATS).* Automation security for ATSs applies to contractor operations as well as Army ATSs. Two key areas of ATSs concern configuration control and the peripheral/system approach.

Configuration control requires that rigid configuration management procedures be established. "Prior to modification, addition, or deletion of any software, firmware, or hardware, a detailed comparison must be made with the approved system baseline. In addition, an analysis will be conducted of all possible effects on system security." Before development or procurement of any ATS hardware/software, it must meet all requirements in security regulations/guidance except when waivers or exceptions apply. Moreover, "interoperation of Army ATSs with those of other DoD or Federal agencies requires an awareness of all applicable security requirements." [Ref. 13: pp. 32]

In the peripherals/systems approach "all system components share the assigned security level. Security considerations must be addressed during development, implementation, and operation of modems, multiplexers, front end processors, remote terminals, video/graphic devices, and input/output devices." [Ref. 13: p. 32]

Other areas covered in Chapter 11 include [Ref. 13: pp. 31-32]:

- ATS responsibilities.
- Processing modes and restrictions.
- Protection of documentation.
- Media security.
- Personnel security requirements.
- Risk assessment and accreditation.
- File access controls.
- Interoperational requirements.
- Maintenance agreements and contracts.

(12) *Appendixes.* The following appendixes apply to LAN security considerations [Ref. 13: pp. 40-69].

- Appendix D - Facility Security Profile (FSP)
- Appendix F - Compilation of Security Protection Guidance for Processing in the Controlled Security Mode.
- Appendix G - Periods Processing Procedures.
- Appendix H - Automation Security Checklist.
- Appendix I - Accreditation Document Format [Ref. 13: p. 58)]
- Appendix J - Privacy Safeguards For Automated Systems.
- Appendix M - Operating System Security Features
- Appendix O - System Vulnerablilities and Penetration Techniques

b. ARMY REGULATION 380-5: Department of the Army (DA) Information Security Program, 15 FEB 85

In sum, "this regulation gives instructions and assigns responsibilities for the effective implementation and application of DoD Information Security Program policies at all levels of DA." For ADP systems in general, this regulation applies to all classified information processed. Understandably, ADP of communications security (COMSEC) is a major concern. [Ref. 20: p. 6]

Classification of information in terms of compilation is one area of AR 380-5 that relates to LANs and ADP in general. Compilation of information is when "certain information that would otherwise be unclassified may require classification when combined or associated with other unclassified information." This is important in research, development, test, and evaluation where each program has a security classification. Compilation areas covered include classification determination, ADP labels, and data formats. [Ref. 20: pp.10-12,19]

A topic directly related to LAN security is transmission of data. Marking of electronically transmitted messages relates to security levels [Ref. 20: pp. 19] Transmission of TOP SECRET, SECRET, and CONFIDENTIAL INFORMATION levels is addressed. Encryption is a major requirement for transmission of data [Ref. 20: pp. 36-37] Exceptions may be authorized by head of the Component (Army, Navy, Air Force, or Marine), if it offers some degree of protection. All exceptions that do not meet the minimum standards in chapter 8 must be approved by Deputy Under Secretary of Defense (Policy) (DUSD(P)). "The ACSI approves exceptions within the Army." [Ref. 20: pp. 36-37]

c. ARMY REGULATION 18-1: Army Automation Management, 15 SEP 80

AR 18-1 sets the framework for policy and responsibility, and delegates authority for Army automation, but does not apply to embedded ADP systems or configurations. AR 18-1 goals include [Ref. 28: p. 1-1]:

- Permit MACOM management flexibility.
- Shorten/streamline acquisition process.
- "Encourage decision making at the lowest practical level."
- "Stress decentralization as a management concept for automation."
- "Insure total systems requirements are integrated to the overall force structure."

Moreover, a valid mission need is required to initiate a project and may be the result of a projected deficiency or outdated system, a change in threat, a technological opportunity, or a chance to reduce operating costs. [Ref. 28: pp. 1-1 - 1-2]

Once a project is under development, "achievement of program goals, rather than time-phased milestones, will be the controlling factor." Other life cycle policies covered include standardization and interoperability, communications support (defined at beginning of system planning), and stand-alone computer management. [Ref. 28: pp. 2-1 - 2-2]

Remaining network related topics, addressed in terms of development costs, are classes of systems, system decision authorities, and authority to acquire administrative systems. Cost estimates must include telecommunications cost and ADP cost. [Ref. 28: pp. 4-0 - 4-1]

d. TECHNICAL BULLETIN TB 18-100: Army Automation Life Cycle Management, 15 Aug 81

TB 18-100 provides a systematic approach to ADP life cycle management by tying life cycle management procedures to requirement documentation and acquisition procedures. It also applies to acquisition and management development of ADP resources and ADP systems that are subject to AR 18-1. TB 18-100 does not apply to systems acquired under AR 1000-1. The objective is to insure that mission program/project objectives and requirements are described in mission terms and not in ADP terms, telecommunications requirements for systems are identified, and automated systems are properly secure. [Ref. 34: p. 2-1]

Planning and documentation topics covered in TB 18-100 do not directly address LAN security. For example, management strategy is mostly related to acquisition. However, standardization and electronic spectrum allocation are two design considerations that relate to LANs and ADP in general. In terms of security, TB 18-100 specificly states that "it is much more expensive and difficult to add security to or introduce security into an already functioning system than it is to include it during the early stages of the life cycle." [Ref. 34: pp. 2-1 - 2-4]

The last point of interest is that telecommunication requirements must be approved according to AR 105-22 before acquisition can be processed. No other major LAN security topics were mentioned. [Ref. 34: p. 3-1]

e. ARMY PAMPHLET 18-4: Processing Installation Review/Evaluation Checklist, 1 SEP 85

This pamphlet is a series of checklists designed to be used by heads of army staff and major Army command automation management offices/officers (AMO), and by DPIs for annual self evaluation audits. The checklists in Pamphlet 18-4 will be used when an equipment upgrade takes place, when a new AMO or DPI manager is assigned, a major reorganization occurs, and in those years when a Department of Army automatic data processing management review is not conducted. [Ref. 24: p. i]

Fifteen major list categories (chapters) are identified by Pamphlet 18-4, within each category sub-checklists exist for specific areas. Categories (chapters) and sub-checklists that relate to LAN security are listed below.

- CHAPTER 1 - GENERAL INFORMATION (addresses Privacy Act of 1974).
- CHAPTER 2 - ORGANIZATIONAL MANAGEMENT
  - Security management.
  - Security planning.
  - Security coordination.
  - Accreditation.
- CHAPTER 5 - AUTOMATED DATA PROCESSING EQUIPMENT (ADPE) OPERATIONS MANAGEMENT (includes Operations Security).
- CHAPTER 11 - DPI FACILITY MANAGEMENT
  - Physical security.
  - Access control.
  - Remote terminal protection.
- CHAPTER 15 - COMMUNICATIONS
  - Network configuration/optimizations.
  - Communications security/emanations security.
  - Remote access security.

f. ARMY PAMPHLET 18-7: Automatic Data Processing Management Review Guide, 3 DEC 85

The purpose of this pamphlet is to assist Army ADP management review teams (MR) in reviewing and reporting on efficiency and effectiveness of Army ADP organizations, and managers who are having their ADP areas reviewed. The objectives are to identify management difficulties, determine the causes of management difficulties, and develop recommendations for solutions to these difficulties. [Ref. 25: p. 3]

In addition, Pamphlet 18-7 also points out that Pamphlet 18-4 is a checklist to be used as a point of reference and that it is just a checklist, nothing more. [Ref. 25: p. 9]

g. ARMY REGULATION 530-2: Communications Security (COMSEC), 1 SEP 82

"The Army's COMSEC goal is to provide total security for all electrically transmitted information from the originator to the recipient." AR 530-2 prescribes responsibility and policy for COMSEC in the Army and implements National Communications Security Directive and DoD Directive 5200.5. Army publications that identify COMSEC responsibilities must conform to this regulation. AR 530-2 applies to all Army units responsible for conducting research, development, test, and evaluation (RDTE) of COMSEC and telecommunications hardware. [Ref. 29: pp. 2-3]

Many areas of AR 530-2 pertain to LAN security; some general points follow. In terms of secure communications, encryption in an approved system is stressed throughout AR 530-2 because encryption is the best defense against foreign exploitation of telecommunications. Yet the regulation points out that "COMSEC measures that are effective today may not be adequate in the future because of advances in COMINT technology. Therefore, COMSEC measures in use must be continuously evaluated." Furthermore, all record telecommunications will be secured by either a protected distribution system (PDS) or encryption in approved cryptosystems. Record telecommunications is defined by AR 530-2 as the telecommunications or teleprocessing of record information. In general, AR 530-2 requires the use of NSA approved cryptographic equipment and commercial communication equipment that meets Federal Standard 1027. [Ref. 29: pp. 2-3]

Clear text transmission of national security information is another area that pertains to LAN security. AR 530-2 "prescribes DA procedures to be used for the unsecured electrical transmission of classified information during emergency situations. It also prescribes criteria under which PDS (formerly known as Approved Circuits) may be established and used for transmission of classified information under a variety of situations." PDSs use physical and electromagnetic safeguards to obtain a secure communications system and is defined by AR 530-2 as a wire line or fiber optic system that permits transmission of unencrypted information. [Ref. 29: pp. 10,15]

h. ARMY REGULATION 18-7: Automatic Data Processing Management Review Program, 30 NOV 84

Besides establishing policies, responsibilities, and procedures for implementing the Automatic Data Processing (ADP) Management Review (MR) Program, it includes review of automation management office installations (AMO), data processing installations (DPIs), and the contractors under their purview. 1 [Ref. 23: p. 2]

AR 18-7 does not contain any specific guidance for LAN security; it contains an overview of topics and a reference to general polices, regulations, and pamphlets that affect management of ADP resources. Topics listed that relate to LAN security are the telecommunication plan, the configuration management plan, physical security communications, and ADP operations.

i. ARMY TECHNICAL BULLETIN TB 18-107: Army Automation Automatic Data Processing Equipment Operations Management, 3 FEB 86

The purpose of TB 18-107 is to implement certain provisions of AR 11-2, provide guidance for general purpose ADPE, and establish standards and prescribe procedures to manage DPIs. The major objectives are to provide DP managers with basic guidance and provide functional staff and management with a basic understanding of ADP operations. [Ref. 27: p. 1-1]

Two specific topics relating to LAN security are data control and ADP equipment sharing. The data control function involves production of "an auditable record of data as if it is routed through the various stages of processing. This concept is important in a service center operation, but it also applies in network environments and distributed systems." Equipment sharing may be done only if the quality or security of mission-related support will not be degraded, and not cost too much. [Ref. 27: pp. 2-1,7-1]

j. ARMY REGULATION 380-53: Communications Security Monitoring, 15 NOV 84

This regulation sets forth, policy, procedures and responsibilities for COMSEC monitoring within the Army. Most of the regulation deals with voice traffic over telecommunications systems. Basic objectives which apply to LAN security include providing information for improving the security of Army telecommunications, and determining the amount of security achieved by US codes, COMSEC techniques, cryptographic equipment and devices, and other related measures [Ref. 30: pp. 3-4] Procedures for determining transmission susceptibility, such as vulnerability and emanation surveys, are addressed. [Ref. 30: p. 5]

k. DEPARTMENT OF DEFENSE (DoD) MANUAL DoD 5220.22-M: Industrial Security Manual for Safeguarding Classified Information, 1 MAR 84

DoD 5220.22-M establishes the requirements for safeguarding all classified information to which contractors have access or possession. It addresses common situations where a contractor needs access to classified information to perform requirements of the contract, and applies to pre/post-contract activity and government sponsored R & D activities. [Ref. 36: p. 1]

One section provides security requirements for ADP systems. In general, "it specifies conditions and prescribes security requirements under which ADP systems will be operated when handling classified information." ADP topics addressed that relate to LAN security are word processing systems, ADP system security procedures, security of remote terminals (including physical disconnects), physical security, and transmission security. Topics for ADP system security procedures include approval, upgrading, downgrading, and media/equipment clearance procedures. [Ref. 36: pp. 171,177-178,184,186-190]

l. DoD DIRECTIVE 5215.1 (DoD Dir 5215.1), SUBJECT: Computer Security Evaluation Center, 25 OCT 82

"This Directive establishes the DoD computer Security Evaluation Center (CSEC), provides policy, and assigns responsibilities for the technical evaluation of computer system and network security, and related technical research."

The policy provided by this directive states that the Consolidated Computer Security Program (CCSP) will include resources for the operation of the CSEC and generic computer security activities of DoD components. In addition, DoD components (Army, Navy, Air Force, and Marines) must perform security research, development, test and evaluation (RDT&E), and application-dependent research and development for, specific DoD component systems. Moreover, CSEC activities and products must complement established responsibilities of DoD components in relation to security, policy, and evaluation of computer systems. Thus, this directive contains only policy guidance for ADP and network security. [Ref. 26: pp. 1-2]

m. DoD MANUAL 5200.28-M: ADP Security Manual Techniques and Procedures for Implementing, Deactivation, Testing, and Evaluating Secure Resource-Sharing ADP Systems, JAN 73

The major objective of DoD 5200.28-M is to provide guidelines, techniques, and procedures to be used to:

- Prevent unauthorized access of classified information.
- Develop, acquire, establish methodologies, techniques, standards, and procedures for design, analysis, test, evaluation, and approval, of ADP systems and components.
- Establish methodologies physical protection of ADP systems and components.
- Prescribe standards, criteria, and specifications for deactivation of secure ADP systems and for sanitization.

The manual states that requirements within it could adversely affect the use of any ADP "system under today's rapidly changing ADP technology. . . This technology is dynamic and the methods chosen to secure a particular system must accommodate new developments without degrading the level of protection." By consequence, the Manual recognizes that techniques described within it may not be economically justified after a cost versus risk evaluation. So, appropriate subsets of the techniques included in this manual, may be used to gain the level of security required to secure a system. Techniques not included can be used if they provide the degree of security specified in DoD Directive 5200.28. [Ref. 22: pp. 1-6]

Topics covered in this manual relating to LAN security include ADP System Security, dedicated and multi-level security modes, remotely accessed resource-sharing computer systems, physical security, communications security, emanations security, hardware and software security features, and audit logs and files. [Ref. 22]

n. DoD COMPUTER SECURITY CENTER CSC-STD-001-83: DoD Trusted Computer System Evaluation Criteria (Also Known as the "Orange Book"), 15 AUG 83

The criteria in DoD CSC-STD-001-83 provides a basis for security effectiveness evaluation of security controls built into ADP systems. The criteria are divided into four broad hierarchical divisions: A, verified protection (most secure); B, mandatory protection; C, discretionary protection; and D, minimal protection (least secure). The criteria objectives:

- "To provide users with a yardstick with which to assess the degree of trust that can be placed in computer systems for the secure processing of classified or other sensitive information."
- "To provide guidance to manufacturers as to what security features to build into thier new and planned commercial products, in order to provide widely available systems that satisfy trust requirements for sensitive applications."
- "To provide a basis for specifying security requirements in acquisition specifications." [Ref. 21: p. v]

Orange Book evaluation criteria labels correspond to AR 380-380 sensitivity labels:

- Verified protection (A) applies to the critically sensitive level (CS).
- Mandatory protection (B) applies to the highly sensitive level (HS).
- Discretionary protection applies to the sensitive level.
- Minimal protection applies to the nonsensitive level.

Two sets of requirements are identified for secure processing: "specific security feature" and "assurance" requirements. Specific security feature requirements are application independent and involve the capabilities usually found in ADP systems that use general-purpose operating systems (separate from applications programs on the system). However, specific security feature requirements may have to be interpreted when applying the criteria to specific applications or special ADP environments. [Ref. 21: pp. v,2]

Assurance requirements apply to all ADP systems and computing environments; from dedicated controllers to full range multilevel secure resource sharing systems. Therefore, no special interpretation is needed for application across any ADP system or application processing environment. [Ref. 21: pp. v,2]

o. **DoD DIRECTIVE 5200.28: Security Requirements for Automatic Data Processing (ADP) Systems, 18 AUG 72**

- Purpose:

1) Set uniform policy to protect classified data stored, processed, used in, communicated, displayed, or disseminated by ADP Systems.

2) In addition to the controls required by the security classification of the material, permit the application of access and distribution limitations imposed on classified data and information.

3) Prescribes security requirements and specify conditions under which "ADP Systems will be operated when handling classified material and assigns responsibility for the testing, evaluation, and approval of such systems."

4) Provide "for the application of administrative, physical, and personnel security measures."

5) Authorized publication of "a DoD Manual of Techniques and Procedures for Implementing, Deactivation, Testing, and Evaluating - Secure Resource Sharing ADP Systems. . . DoD 5200.28-M." [Ref. 32: .pp 1-2]

- Objectives - to establish that:

1) ADP system security controls are interrelated with normal system controls.

2) System security requirements/controls enhance the reliability, integrity, and operation of an ADP System.

3) "The basic ADP system reliability and integrity features prevent unauthorized access and manipulation with reasonable dependability. [Ref. 32: .p 2]

Topics covered in this manual relating to LAN security include ADP system security, dedicated and multi-level security modes, remotely accessed resource-sharing computer systems, physical security, communications security, and emanations security. [Ref. 32]

p. **NATIONAL COMPUTER SECURITY CENTER PUBLICATION NCSC-WA-002-85: Personal Computer Security Considerations, 1985**

This publication addresses issues that are pertinent to microcomputer security in the home and business environment. It is NOT a formal government policy document, but rather an information memorandum. [Ref. 33: p. i]

NCSC-WA-002-85 notes that personal computers offer an unlimited opportunity for intrusion into mainframe computers and networks (assuming the PC has communication hardware/software). It indicates that transmission of sensitive information from a PC to another device is the responsibility of the user. In terms of communication security, dial-back procedures are considered questionable, with encryption identified as a "sure method" of protection. Dial-back procedures cause the PC to disconnect the caller, check a list of authorized IDs, and call back. [Ref. 33: pp. 8,11]

Again, PC data transmission and communication attacks are addressed in the publication. However, the publication is most concerned with security of a stand-alone PC. [Ref. 33: p. 1]

LIST OF REFERENCES

1. Schell, Roger R., Lt Col, USAF, "Computer Security the Achilles' of the Electronic Air Force?" *Air University Review*, Vol. XXX, No.2, pp. 16-33, January-February 1979.

2. Defense Investigative Service, Department of Defense, *Computer Security Security Awareness Circular*, DoD 5220.22-M, Defense Security Institute, Richmond, VA, January 1986.

3. *Websters New World Compact Dictionary of Computer Terms*, Simon and Schuster, Inc., New York, 1983.

4. Stallings, William, *Tutorial Local Network Technology*, IEEE Computer Society Press, 1983.

5. Dupuy, T. N., Col USA, Ret., *In Search of an American Philosophy of Command and Control*, preliminary draft, OS3636, Architecture of C3 Information Systems, course handout, Naval Postgraduate School, Summer Quarter, 1986.

6. Wohl, Joesph G., "Force Management Decision Requirements for Air Force Tactical Command and Control," in *IEEE Transactions on Systems, Man, and Cybernetics*, Vol. SMC-11, No. 9, pp. 618-638, September 1981.

7. Rullo, Thomas A. (ed), *Advances in Distributed Processing Management Volume 1*, Heyden, 1980.

8. Cheong, V. E. and Hirschheim, R. A., *Local Area Networks Issues, Products, and Developments*, John Wiley and Sons, 1983.

9. Ulmen, Patrick A., "The Impact of Commercial Computer Technology on C3I." *Signal*, pp. 67-72, March 1985.

10. Foss. Ronald W., "Processing Environments for Dispersed Command and Control," *Signal*, pp. 87-93, April 1986.

11. Lackey, R. D., "Penetration of Computer Systems - An Overview," *Honeywell Computer Journal*, Vol. 8, No. 2, pp. 81-85, September 1974.

12. Prevention Committee President's Council on Integrity and Efficiency, *Computers Crimes, Clues and Controls, U.S. Government Printing* Office, Washington, D.C., March 1986.

13. Department of the Army, Headquarters, *Automation Security*, Army Regulation 380-380, U.S. Government Printing Office, Washington, D.C., 8 March 1985.

14. Stallings, William, "Local Network Overview," reprinted from *Signal*, January 1983, in *Tutorial Local Network Technology*, pp. 7-11, IEEE Computer Society Press, 1983.

15. Wood, David C., "A Cable-Bus Protocol Architecture," reprinted from *Proceedings of the Sixth Data Communications Symposium*, November 1979, in *Tutorial Local Network Technology*, pp. 186-194, IEEE Computer Society Press, 1983.

16. Stallings, William, *Data and Computer Communications*, Macmillan Publishing Company, 1985.

17. Rosenthal, R., "Transmission Media," *The Selection of Local Area Computer Networks*, reprinted from NBS Special Publication 500-96, November 1982, in *Tutorial Local Network Technology*, pp. 19-34, IEEE Computer Society Press, 1983.

18. Shoch, John F., and others, "Evolution of the Ethernet Local Computer Network," reprinted from *Computer*, August 1982, Institute of Electrical and Electronics Engineers, Inc., in *Tutorial Local Network Technology*, pp. 39-54, IEEE Computer Society Press, 1983.

19. Department of Defense Computer Institute, course material from "Managing Automated Information Systems Resource Protection, (RP-2-86)," National Defense University, Washington Navy Yard: November 1985.

20. U.S. Department of the Army, *Information Security Program*, Army Regulation 380-5, U.S. Government Printing Office, Washington, D.C., 15 February 1985.

21. Computer Security Center, Department of Defense, *Department of Defense Trusted Computer System Evaluation Criteria*, CSC-STD-001-83, U.S. Government Printing Office, Washington, D.C., 15 August 1983.

22. Assistant Secretary of Defense (Comptroller), *ADP Security Manual Techniques and Procedures for Implementing, Deactivation, Testing, and Evaluating Secure Resource-Sharing ADP Systems*, DoD Manual 5200.28-M, U.S. Government Printing Office, Washington, D.C., January 1973.

23. U.S. Department of the Army, *Automatic Data Processing Management*, Army Regulation 18-7, U.S. Government Printing Office, Washington, D.C., 30 November 1984.

24. U.S. Department of the Army, *Data Processing Installation Review/Evaluation Checklist*, Pamphlet 18-4, U.S. Government Printing Office, Washington, D.C., 1 September 1985.

25. U.S. Department of the Army, *Automatic Data Processing Review Guide*, Pamphlet 18-7, U.S. Government Printing Office, Washington, D.C., 3 December 1985.

26. Deputy Secretary of Defense, *Computer Security Evaluation Center*, DoD Directive 5215.1, U.S. Government Printing Office, Washington, D.C., 25 October 1982.

27. U.S. Department of the Army, *Automatic Data Processing Equipment Operations Management*, Technical Bulletin 18-107, U.S. Government Printing Office, Washington, D.C., 3 February 1986.

28. U.S. Department of the Army, *Army Automation Management*, Army Regulation 18-1, U.S. Government Printing Office, Washington, D.C., 15 September 1980.

29. U.S. Department of the Army, *Communications Security*, Army Regulation 530-2, U.S. Government Printing Office, Washington, D.C., 1 September 1982.

30. U.S. Department of the Army, *Communications Security Monitoring*, Army Regulation 380-53, U.S. Government Printing Office, Washington, D.C., 15 November 1984.

31. *Websters Ninth New Collegiate Dictionary*, Merriam-Webster Inc., 1984.

32. Deputy Secretary of Defense. *Security Requirements for Automatic Data Processing (ADP) Systems*, DoD Directive 5200.28, U.S. Government Printing Office, Washington, D.C., 18 December 1972.

33. National Computer Security Center, *Personal Computer Security Considerations*, NCSC-WA-002-85, U.S. Government Printing Office, Washington, D.C., December 1985.

34. U.S. Department of the Army, *Army Automation Life Cycle Management*, Technical Bulletin 18-100, U.S. Government Printing Office, Washington D.C., 15 August 1981.

35. Brown, Thomas J., Maj, USAF, instructor, course lecture material from Telecommunication Networks, CM4502, Naval Postgraduate School, Winter Quarter, 1987.

36. Defense Investigative Service, Department of Defense, *Industrial Security Manual for Safeguarding Classified Information*, DoD 5220.22-M, U.S. Government Printing Office, Washington, D.C., 1 March 1984.

37. Sidhu, Deepinder P., Gasser, Morrie, "A Multilevel Secure Local Area Network," reprinted from *Proceedings of the Symposium on Security and Privacy*, April 1982, in *Tutorial Local Network Technology*, pp. 281-287, IEEE Computer Society Press, 1983.

38. Dietz, Lawrence, Capt, USA, "Microcomputer Security," *C2 Mug Bulletin*, Publication of the Command Control Microcomputer Users Group, Communications-Electronics Command, Vol. VI, No. 9, pp. 4-6, December 1985.

39. Chorafas, Dimitris N., *The Handbook of Data Communications and Computer Networks*, Petrocelli Books, 1985.

40. Naval Electronics System Command, Naval Research Laboratory, *An Approach to Determining Computer Security Requirements for Navy* Systems, by Carl E. Landwehr and H.O. Lubses, 13 May 1985.

41. Broestl, Howard E., Maj, USAF, *Security Implications of Local Area Networks (LAN)*, paper required for graduation from Air Command and Staff College, Air University, Maxwell AFB, 24 October 1984.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5002	2
3.	Department of the Army Director, USA Combat Developments Experimentation Center Attn: ATEC-IM (Mr. R. Davis) Fort Ord, California 93941-7000	1
4.	Department of the Army Director, USA Combat Developments Experimentation Center Attn: ATEC-IM (CPT Peter J. Blakney Jr.) Fort Ord, California 93941-7000	2
5.	Department of the Army Director, USA Combat Developments Experimentation Center Attn: ATEC-IM (Technical Information Center) Fort Ord, California 93941-7000	1
6.	Thomas J. Brown, Maj, USAF, Code 62Bb Department of Electrical Engineering Naval Postgraduate School Monterey, California 93943	1
7.	Joint Command, Control and Communications Academic Group Code 39 Naval Postgraduate School Monterey, California 93943	1
8.	Jeffrey D. Ayres, Capt, USAF Box 1893 APO, New York 09021	4
9.	Michael G. Sovereign, Code 74 Joint Command, Control and Communications Academic Group Naval Postgraduate School Monterey, California 93943	1

END

7-87

DTIC